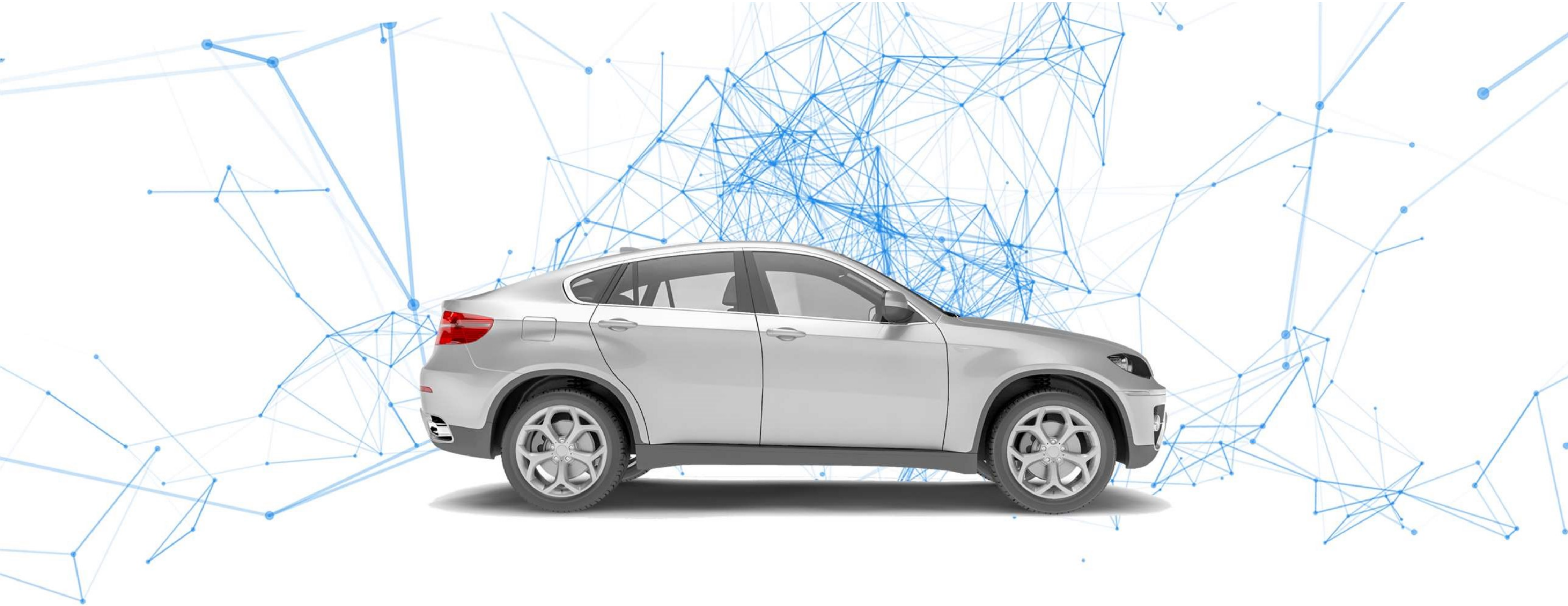


DoIP (ISO13400) Enhancements for Future Architectures

IEEE SA Ethernet & IP @ Automotive Technology Day 2020

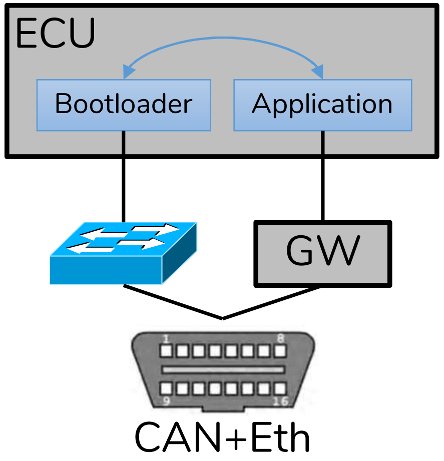
Max Turner

History

BMW’s High-Speed Vehicle Access

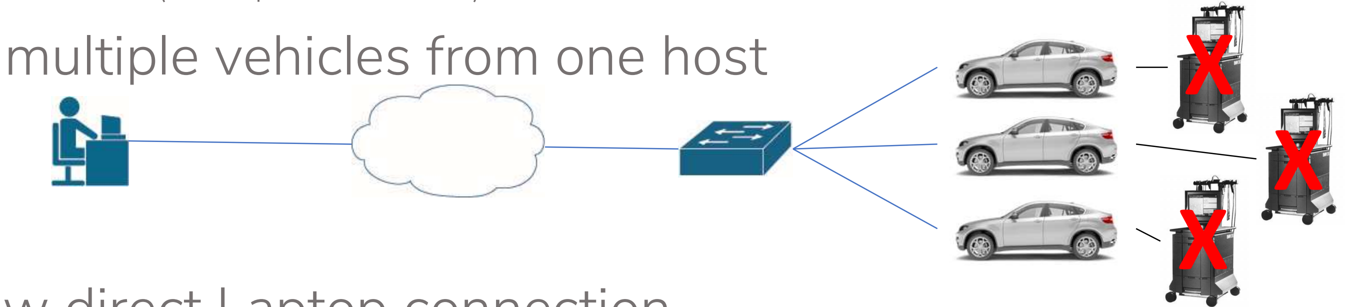
- Flash-Update via Ethernet only
  - Diagnostics running over CAN (Gateway required)
  - Few high update-volume ECUs get two connections
  - Direct Layer 2 connection in Programming-Session only

- Ethernet as “System-Bus”
  - One physical Ethernet link per ECU with 2 VLANs
  - Diagnostics running over internal VLAN (Gateway required)
  - Direct Layer 2 connection in Programming-Session only



The Original Goals of ISO13400

- Remove the Gateway - decentralized per ECU approach
- Reduce the time to update vehicle software
  - Remove the in-vehicle SW-Gateway from the update-path for ECUs connected to Ethernet
- Access the vehicle from a remote host via Ethernet and IP infrastructure
  - Remove the (one per vehicle) CAN-tester
- Access multiple vehicles from one host



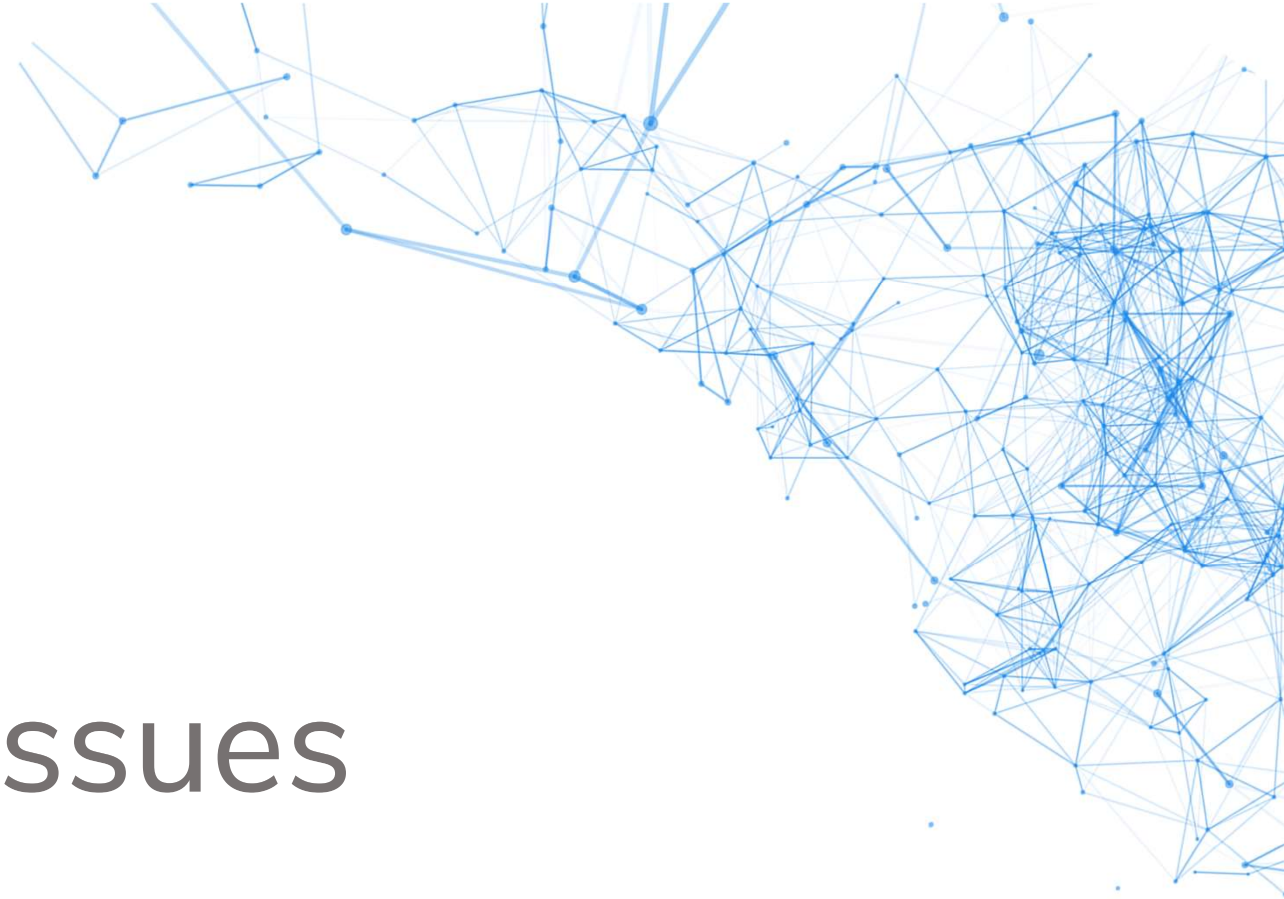
- Still allow direct Laptop connection

Did it work? – Well ...

- High load on DHCP servers (assembly plant)
- AutoIP wait times as PC starts DHCP first
- Keeping
  - ECU (UDS address)
  - TCP session (MCD-3D limitations)
  - IP address
  - vehicle (VIN)

  aligned proved difficult

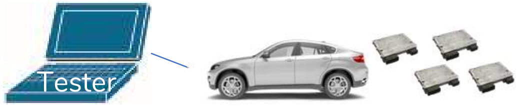
- Growing safety (engine-ECU reset while running) and security (OBD dongles) concerns

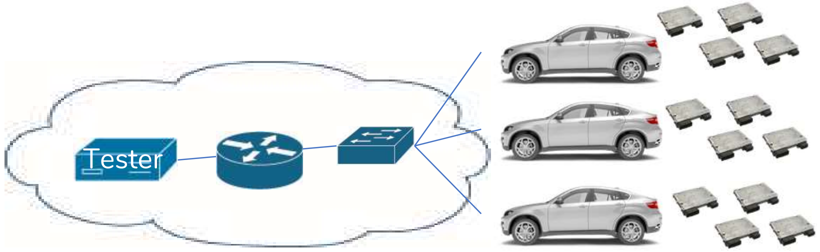


Addressing Issues

UDS-Server (ECU) Discovery Issues

- Given there are n vehicles on an assembly line or in a workshop, with m ECUs per vehicle, there may be 3xn×m vehicle announcement messages broadcast within 1.5 seconds



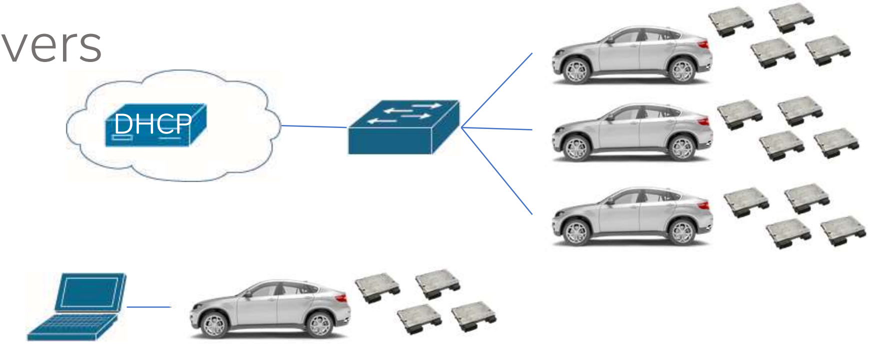


- This works well for a directly connected laptop but is likely hugely inefficient in an unknown network infrastructure

- As announcements can only be sent after IP Address Assignment, the discovery process is slow and unreliable with unintended consequences (time-out, message load, …)

IP Address Assignment issues

- Given there are n vehicles on an assembly line or in a workshop, with m ECUs per vehicle, there will be n×m DHCP (IPv4) requests within a short time
- ISO13400 has no requirements on DHCP-servers



- On a Laptop DHCP, starts before AutoIP
- ISO13400 has AutoIP settings for ECUs only
- Do all ECUs need to support IPv4 and IPv6?
- IP Address Assignment is slow and has unintended consequences (time-out, security, ...)

Globally unique MAC Address Scarcity

- Just like with IPv4 addresses, we see a scarcity of globally unique MAC addresses
- A node, which is exposed to an unknown network infrastructure must use a globally unique MAC address in order for switches/bridges to function properly
- ECUs see unknown network infrastructure only very few times during their life-cycle:
  - during testing
  - end of line software distribution
  - DoIP flash update in service
- Are we wasting MAC address space?

Vehicle Internal Communication

Vehicle Internal Gateways

- A ”vehicle announcement message” can map one single IP-address to one single logical UDS-address (with a common default port)
- A DoIP to CAN Gateway would potentially have to send one ”vehicle announcement message” per CAN node
- If functions are to be deployed on more complex integrated ECUs (including hypervisors), the concept of one logical UDS-address per “ECU box” may go away and logical UDS-addresses may be assigned to functions
- The diagnostic vehicle announcement and discovery concept may need to look more like a service discovery

Internal Tester is Required

- ISO13400 assumes the internal test equipment to be "optional" (section 6.2.3)
- This seems inaccurate as diagnostics via the OBD-CAN connection via a Gateway will result in a de-facto internal tester for all ECUs not connected to CAN
- While section 6.2.3 mentions "static IP address configuration", it does not make provisions for how to use these (VLAN?) these, how to switch between connections and how to do IP- to logical-address mapping
- There are no exceptions e.g. for "alive check" when using internal test equipment

TCP connection handling

Reconnection after an ECU-Reset

- During the Flash-Update process an ECU will go through reset at least once, breaking up the TCP connection
- Currently many testers start sensing connection requests after a “reset timeout”. As these go to the same IP address, but the ECU needs to go through DHCP/AutoIP during boot-up, the ECU may no longer be reachable
- A vehicle internal GW needs to make sure it frees the resources taken up by terminated TCP connections, so the reconnection can succeed
- The reset of Switch-ECUs may terminate the reachability of any number of ECUs behind the switch/bridge

Error Handling

- DoIP has many error cases, where the TCP connection is terminated by the ECU, e.g. due to a duplicate tester address (after Alive-Check) or an unknown Payload-Type

- This is not very practical for a GW, where multiple Tester-to-ECU links may run over one single TCP connection

- It has proven difficult in a middleware environment where an application has limited control and knowledge over (limited) network resources

UDS over TCP

- TCP was chosen as the Layer 4 protocol, because DoIP was tailored to the flash-update use-case
- TCP timeouts do not fit well with UDS timeouts
- TCP has limited hardware support, limiting CAN to TCP gateway efficiency
- TCP resource and session handling is cumbersome

- TCP is perfect to deliver data through the internet to the vehicle!
- But: Is TCP the right protocol to distribute data inside the vehicle?

Security

Edge-Node Security

- The dynamic address assignment and per ECU announcements require opening communication through the switch in the Edge-Node

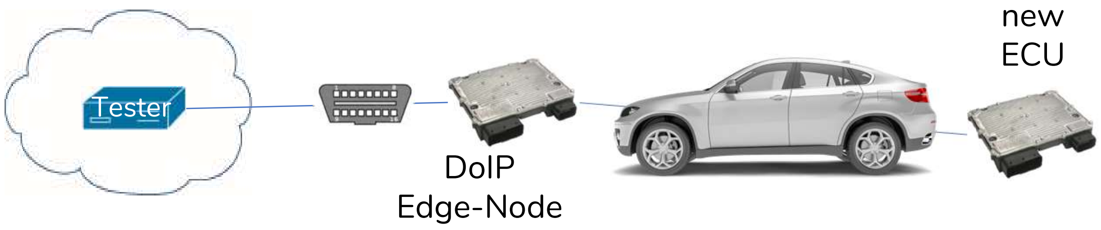
- Trust between ECU, Test equipment and Vehicle is currently completely unrelated

- Smarter communication and situational awareness can e.g. allow the Edge-Node to set up filters in hardware

New ECU Integration

- If a new ECU is fitted to a vehicle, e.g. during repair in a workshop, there may be a need to update the software of the ECU, before it can communicate with the rest of the vehicle - This update may include key material

- Hardware support, e.g. of IEEE802.1X and IEEE802.1AE, along with smarter discovery can help isolate untrusted traffic flows through the vehicle



Summary

Conclusion

- The idea of a decentralized per ECU diagnostics flash access did not hold up with the increase in Ethernet-only connected ECUs
- The vehicle internal diagnostics communication is currently not sufficiently reflected in ISO13400
- There is no DoIP specification for test equipment, taking into account the ASAM MCD-3D standard
- Just going back to a software-gateway solution seems inefficient
- Smarter hardware solutions require a smarter protocol

⇒ A system description covering internal and external test equipment, ECUs as well as network infrastructure is desirable

THANK YOU

ETHERNOVIA | max.turner@ethernovia.com