Pairing I

What are the pros and cons of NFC for pairing (tag vs. bidirectional, functional safety, production/use/repair etc.)?

5 min notes, 5 min review

Intro to Mural:
- Navigate Outline on the right
- Keep "space bar" pressed to move more
MURAL without dragging objects
- Ctrl + Z to undo
- Right click to add sticky note OR grab o
- Use sentences if possible
- Add your initials/name if possible

PRO
No Tag required. The security / codes are stored in the main control unit of the vehicle. "Outside" is only the antenna.

pro: NFC can be re-used for communication in addition to pairing -> low BOM/cost

Pay attention : NFC as trademark vs multiple declinations and standards for short range use of RFID

pro: short wireless range = easy security

PRO - Due to mehcanical mating / alignement of nozzle NFC will be reliable

PRO - NFC wireless is intrinsically safe

Pro: Commonly used technology

pro widely used.
low cost

Almost certain peer / peer identification

Ultra short range of only a few cm. Bluetooth accuracy of 1m is not short enough.

Pro: NFC tags can be tamper proof. (Signed by manufacture.)

? what are the estim. IPR licensing costs for NFC?

Pro : integrated anti-tamper more and more common

To be secure and avoid NFC tag replacement, one solution is to separate the ECU from the NFC antenna

con: short wireless range - mechanic restrictions (moblity, 360° rotation, temperature, wear-off)

possible cable damage with NFC in nozzle

Con: May need to be classified electrically

PRO NFC + wireless communication uses two independent systems, therefore best for safety against steeling of NFC and against hacking of the vehicles software, data of both can be compared by station

Pro/Con: What is SIL rating?

Con: Often does not work reliability

Con: requires wire or antenna which can fail

Couple NFC pairing with wieght-based confirmation of vehicle presence in front of the dispenser ?

CON: If using external data for confirming vehicle ID, NFC may require as much time as credit card transaction (and adding to fueling time) - longer range technology may allow for additional time for ID confirmation (basically, vehicle can already been ID'ed when entering fuel station area)

Pro:
NFC is easy and safe. It is easy guaranteed that the pairing is correct

PRO - Data stored on NFC tag can be encrypted and vehicle specific

PRO - NFC tag is easy to replace if a vehicle requires collision repair.

Possibly very limited and controllable amount of EM radiation in close vicinity of the gas eschange point

Pro: commonly used, short range, bidirectional possible as backup in case 5G fails, cable on nozzle will be easy to integrate (nozzle will likely be a significant size).

NFC for pairing only -> OOB exchange of info w/r to filling data

can it be considered as a safe (SIL) connection

Con: May be ok for vehicle ID, but not tank ID

Con : com may be hindered by water droplets / freezing

if used onlyl for Pairing, a second wireless technology is necessary to do the data exchange.

Tag / reader vs bidirectional : lesser surface of attack ?

cons: possible loss of connection during fueling process

To be secu avoid NFC tag replacement, one solution is to separate the ECU from the NGC antenna

I have no idea, but it is OK to use NFC at extreme cold temperatures?

Cons NFC: NFC reader on the Nozzle, need a cable, that is not very confortable for the user.

PRO - Cost imapact of adding NFC tag to vehicle is low

PRO - NFC is not susceptable to RF interference common to long range RF technology

PRO
NFC is a known technology. It is used for payment, access, other security things an encryption. It is a short range P2P communication.

PRO
Realtime communication with low latency. (In contrast to WiFi or Bluetooth)

What about : tag on the dispenser, reader and responsibility of pairing on the vehicle ? (eliminates faulty cables on the dispenser)

Can the transmitter/receiver be located further back on the nozzle, or even on the hose assembly instead (also to avoid risk of damage when dropped) - if so this would be better presumably than images shown yesterday with the technology on the end of the nozzle, like the current IrDA technology

PRO
No interruption or disturbance due to short range. Long range communication can be disturbed by hackers.

How about the impact of electromagnetic interference using NFC?

Cons: Need to design new nozzle

PROS

CONS

Pairing III

If NFC, which solution do you prefer?

NFC tag (pairing) plus wireless network (fueling data exchange)

bi-directional NFC only (pairing + fueling data exchange)

vehicle OEM

station manufacture
operator

either outside
or at the edge of
the scope

Custom short-range, non propagating wireless but not based on RFID / NFC framework

5G

DSRC - Decicated Short Range Comms

Human operated PIN & Chip

Cell phone pairing with cell phone towers

Pairing II

Are there alternative solutions to NFC for pairing?

5 min notes
10 min review
+ grouping
3 min ranking

RuBee

current IRDA ?

Continue using the IrDA

Because of the short distance I see no real alternative exept IrDA

Optical scan

Visual ID of license plate

Vehicle plate recognition ?

RFID with localization

RFID (previously tested)

Combination with mechanical foolproof confirmation of contact

wired connection plug

Electrical contact / electrical plug

direct cable/plug connection similar to loading station for BEV

Customized impedance detection ?

NFC
Not aware of any suitable alternatives that match the performance of NFC

No!
Don't see a compelling alternative to NFC.

Localisation by localisation through BLE

Bluetooth 5.1+ and Trianglulation/ Trilateration

Wireless location methods (RSSI triangulation, AoA, etc..)

put vehicle key to NFC reader @ dispenser, has often vehicle information included already

Ultra-Wide band (UWB): different "standards": IEEE 802.15.4c, ECMA/ ETSI TS 102 455; Apple

Localisation by localisation through UWB (Solution choose by Apple & Samsung)

Utilize dispenser measurements,

Wireless Communication - What are pros/cons of the diffe

Bluetooth

No impact on the nozzle & on vehicle

Strong Relability

Existing technology which is commercially available and mature

already on-board on vehicle (entertainment, tire pressure)

Fast evolving standards / protocols (driven by customer Xtronics innovation) -> is this a good bet for long-term support and maintenance ?

Provide cost benefit over NFC

Robust (no hardware for user to damage)

Strong Relability

Low energy consumption

resistant to emc interference

standalone

High Safety Integrity Level (SIL3)

Mature technologie and very easy

Inexpensive

low IPR costs

precise localization possible

Very low latency (3-10 ms)

Mature, existing, widely used technology in vehicles for communication between vehicle and cell phones, headsets, computers (after initial pairing confirmation through a 4 digit code)

After pairing will exclude other devices

Forward Error Correction allow the receiver to detect errors and recover the original data without the need to retransmit the data

PROs

High density of devices using this technology (interferences)

the distance control unit location inside the vehicle - filling station my be to long for bluetooth

high prob. of interference with WiFi (mobile phones, laptop PCs, etc.)

Strong end-to-end coupling at functional and security level between the vehicle and the station

Sensitive for disturbance e.g. by hackers

Co-existence with infotainment

what license? intell. property; spectrum license?

I "think" BT needs a license

Yes, needs BT certifcation and stamp at the product-family level

Fees and licensing will always apply

CONs

NFC bi-directional

Safe communication (PROFIsafe, black channel)

Safe comms, easy to adapt to nozzle/ receptacle

standalone

supported bandwidth high enough for all use cases? Answer: up to 424 kbit/s, current RDI: 38.4 kBit/s

Datarate should be ok for the filling step

It is the only technology which allows a seperation of control unit and antenna

wires - NFC Tag - control unit are less critical becaus of the lower frequencies compared to the other options

Unidentified

PROs

Cost impact to vehicle to add NFC for fueling. Safety certification required for black-channel use.

Strongest end-to-end coupling at functional and security level between the vehicle and the station

Hardware impact (space requirements)

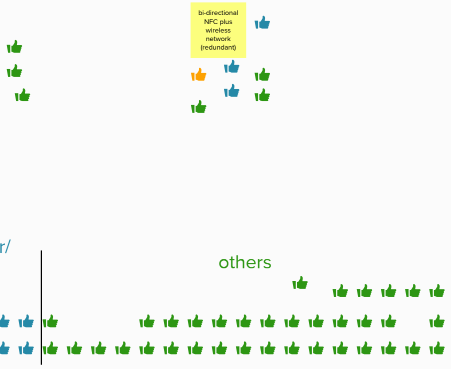
Need a cable between the nozzle and dispenser

Strong impact on the nozzle & on vehicle

mechanic restrictions: antenna at nozzle

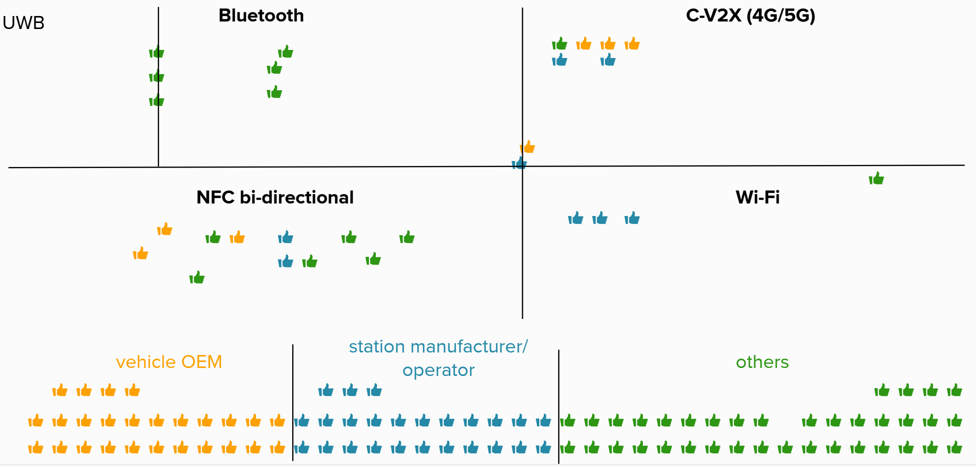
CONs

3min ranking
10min discussion



Key Question: What is your preferred wireless communication standard?

3' ranking
15' discussion



erent network standards below?

15 min notes
10 min review

C-V2X (4G/5G)

PROs

third-party supervision, admin. and spectrum management, SLAs

Additional services more easy to develop

Access to cloud resources for optimal supervision

Long support

Is a cheap option due to synnergy of H2 refueling communication and other use of 4G/5G.

HD trucks will likely already use this technology

Better functional de-coupling between station and vehicle

Useful for 3rd-party trust authority

Commonly available on vehicles

Cheap solution if future trucks are equipped with for contact to their main station

5G slicing may be of interest for granted / truste operations

CONs

Station control depends on other facility.

Deployement / ramp-up / decomissioning are country and operator based

operating fees

Costs

The Filling control unist is located somewhere in the vehicle and high frequency antenna wires are expensive

The antenna must be kocated outside the vehicle - expensive antenna wire necessary

Wi-Fi

PROs

Commonly used

Together with NFC for redundancy

standalone

already available onboard on vehicle (entertainment)

Only requires a local peer-to-peer connection between vehicle and dispenser.

CONs

Coexistence with (many) other WLANs in the area is critical

Un-licenced frequency bands -> jamming & legal issues ?

non-managed network -> crowding ?

The antenna must be mounted at every vehicle on the same are to ensure correct pairing

kinda strong end-to-end coupling at functional and security level between the vehicle and the station

Wifi very easy to hack

Ubiquitous

hig IPR licensing costs

high prob. of interference (mobile phones, laptop PCs, Bluetooth etc.)

Does not rely on cell infrastructure

WiFi certifcation and stamp required at the product-family level

Authentication I

5 min notes
5 min review

How can trust be established between the vehicle and the dispenser for safety-critical communication? What are existing solutions used today?

Actually it's not trustable. Because even in safe communication, ECU or sensor might have wrong. Ex. Illegal modification or something.

Compare ID of short range and long range communication

Secure NFC (as used by credit card companies)

Payment technologies

Use NFC to identify the vehicle and identical identify information comming from TCU by independant communication, to be compared at the station

Use of unique identifier per Hydrogen tank and of a central global accessible database

Temporary idenitifiers (last only for filling session duration)

Embedded tank/CHSS ID (unique DNA)

Use of encryption and certificate authorities.

Dispenser can monitor changes in vehicle pressure/temperature and verify that they match expected changes

Challenge of the vehicle by the station + challenge of the station by the vehicle

use of secure elements / bastion components

Vehicle number plate recognition, with data sent to central database, and back out again to dispensing unit

Provide certificat to the vehicle and to the station, then Challenge–response authentication (well known

Double-blind challenge by a 3rd party authoirty / a component in the middle

Robustification by 1 Out Of Bound element (e.g user input on dispenser IHM)

Correlating the location of the pairing data emission point with the location of the auth. data emission point

Vehicle can transmit SIL level of information that is transmitted as part of packet

EMV standard/ method (to establish trust)

Block chain solution

Can blockchain be implemented somehow?

Authentication II

Do modern vehicles carry a unique ID for safety-critical tasks that can be used to uniquely identify them? In what systems/applications is it used?

5 min notes
5 min review

Vehicle should not have safety critical info.
It make vehicle expensive. If Illegal modification by user occur it may make mismatch. Then station get fail.
The latest LDV refueling technology already has achieved 4 times higher APRR than L/T. No need to have critical info on vehicle.

GPS identifier

If vehicle is able to contact it´s home via 4G/5G there will be a unique ID

Same as main control unit the TCU may have a unique ID together with best knowledge about present tank system

Can't comment with OEM perspective... but use of globally unique identifiers in electronics is pervasive and cost pennies. Third-party certificates are also globally unique. Block chain... many potential solutions.

Im no expert here, but I know the German "Fahrgestellnummer"

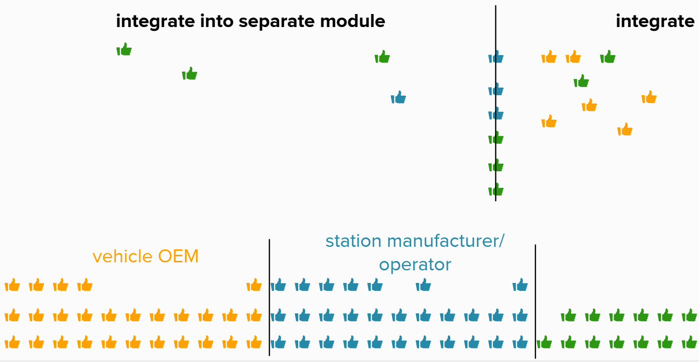
There is the VIN number saved in the main control unit.

VIN => Vehicle Identification Number (Fahrgestellnummer). However, there may be a concern about after-sales (HSS replacement) to be managed

VIN

E/E architecture

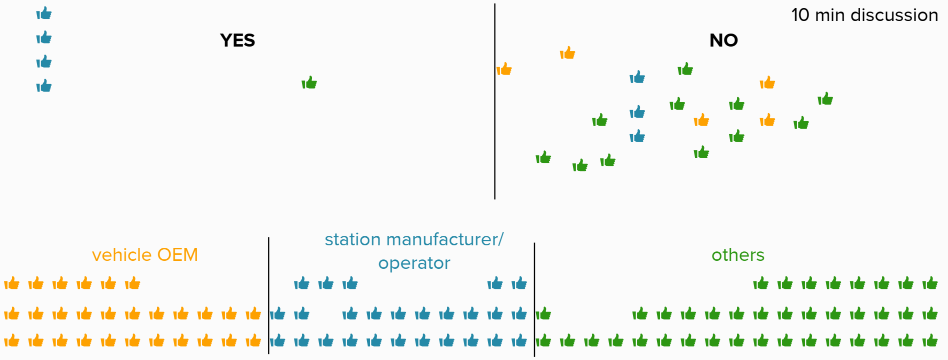
Do you think a separate communication module should be inserted to the E/E architecture or should the dispenser-communication be integrated into an existing control unit?



Authentication III

Is a third-party authentication service acceptable?

3 min ranking
3 min review
10 min discussion



Comments left in MURAL comment section

There was a suggestion that the comms technology needs to be ATEX rated for Zone 1 for one part, and zone 2 for another (and presumably the equivalent to ATEX / IEC Ex in other regions) - is there somewhere that defines this need?

Where do the current restrictions on how communicated data can be used by the station in defining the refuelling protocol come from? Are they choices made by station manufacturers, or driven by station permitting bodies/authorities? (Just to understand whose assessment of how data is communicated is critical to permit this for the future...)As an example, my understanding is that AP already treat IR comms as safety related as will use a lower target pressure than the SAE non-comms tables if there are no comms? Also, it isn't clear to me which dispenser manufacturers use the option in J2601 to use the communicated CHSS category, and why they can use it, where others can't (is it based on the mass flow meter accuracy for the initial pressure pulse for instance?) - or is it simply down to acceptance of risk by the dispenser designer?

How the grounding discussion affect the pairing discussion?

We need to make sure we learn from the issues in the field today

What's the fallback strategy? If none, will vehicle NOT be filled if not ID'ed/ authenticated/ verified?

How could different options exist and operate in parallel?

What are the similarities of the issue at hand with autonomous vehicle identification/authentication?

What are the next step for Hyconnect and also for the participant of this workshop?

3 min ranking
10 min discussion

into existing ECU

others

Closing thoughts

What are your most important take-aways? What areas need the most work?

min notes
min vote

Repartition of preferences along the safety vs simplicity axis
-> need to consider also : simplicity of a single dispenser vs. a country grid of dispenser
-> ventilation of legal responsibilities / accountability according to the different architectures

Maybe we focused to early on some peculiar technology, a roll-back to the presented functional views / user stories / lifecycle assessment could be useful

These discussions were very fruitfull, but also very confusing und sometimes wrong. An analysis (safety, hazard etc.) has to be performed with experts in their fields providing reliable results.

Take away=> great to have a project like this preparing the grounds for the standardization process.<div>Most critical area of work => deciding and agreeing on the data to be shared during fueling and agreeing on the responsibility share (Vehicle /Station) </div>

The discussion about tank control unit was very interesting and insightful. Thanks a lot.

Define the authentification procedure, type, medium, ..; will need further discussion. Part of those discussions should not necessarily be done with hydrogen experts but find autonomous driving experts, which certainly have similar challenges

One big challenge is to find an agreement on the communication technology, without closing doors, especially for the future as experienced for IR

introduction of communication also with respect of already existing vehicles on the road

There are ways to avoid an additional part for pairing (NFC tag).

work on solution cost

This meeting was helpful to understand how very far we still need to go before we will be ready to create a standard

Need to TEST the options, since there was no clear winner and loser (in theoritecal discussions)

There's a lot more work to do for this generation of communications, but we need to remember that we are transferring data between two pieces of hardware safely and reliably

Please join the ISO TC/197 19885-2 Advanced Comms meeting.
We are looking for presenters!

Unclear what the fallback strategy is (vehicle ID fails)

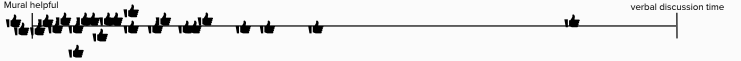
As long as mechanical Poka Yoke between tank and station is realized, no wrong System can be filled. Therefore we are only talking about the chance for faster refuelling. If station realizes that with first pressure test the vehicle gives wrong answer fallback to slow refuelling ist possible

How dow we get everyone to a common understanding of the base issues? Bring everyone up to speed?

do not re-invent crypto / authentication ! --> need for specialists ?

How does this apply to other than gaseous H2?

Vote:



5min notes
10 min review