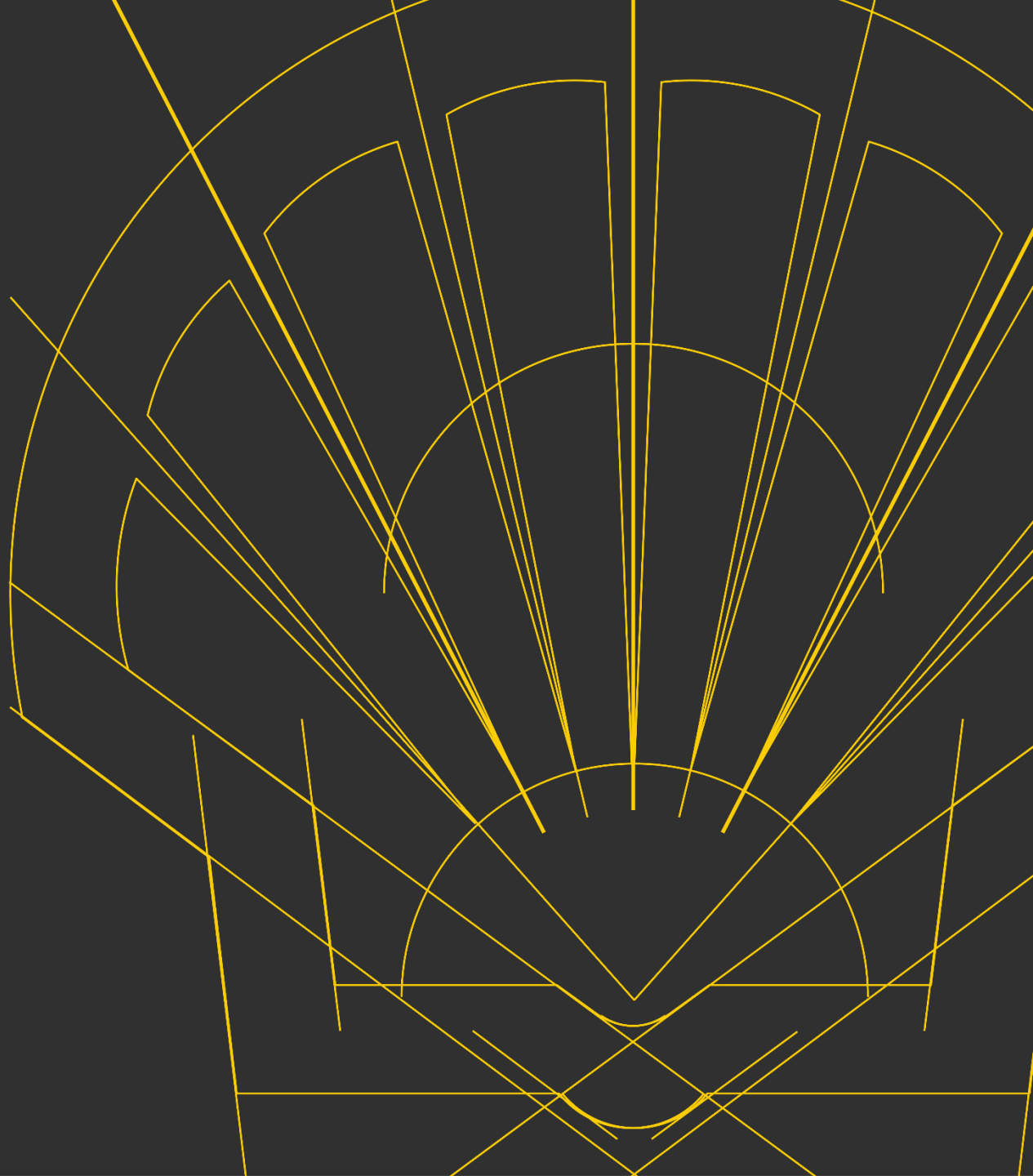
TECHWORKS

HyConnect - Wireless Communication Between H2 Vehicles and Dispensers

Ulrich Muecke | Product Development Fellow
contact for questions: Benoit.Poulet@shell.com | OEM interface manager
Jul 22-23, 2021, CEP Workshop



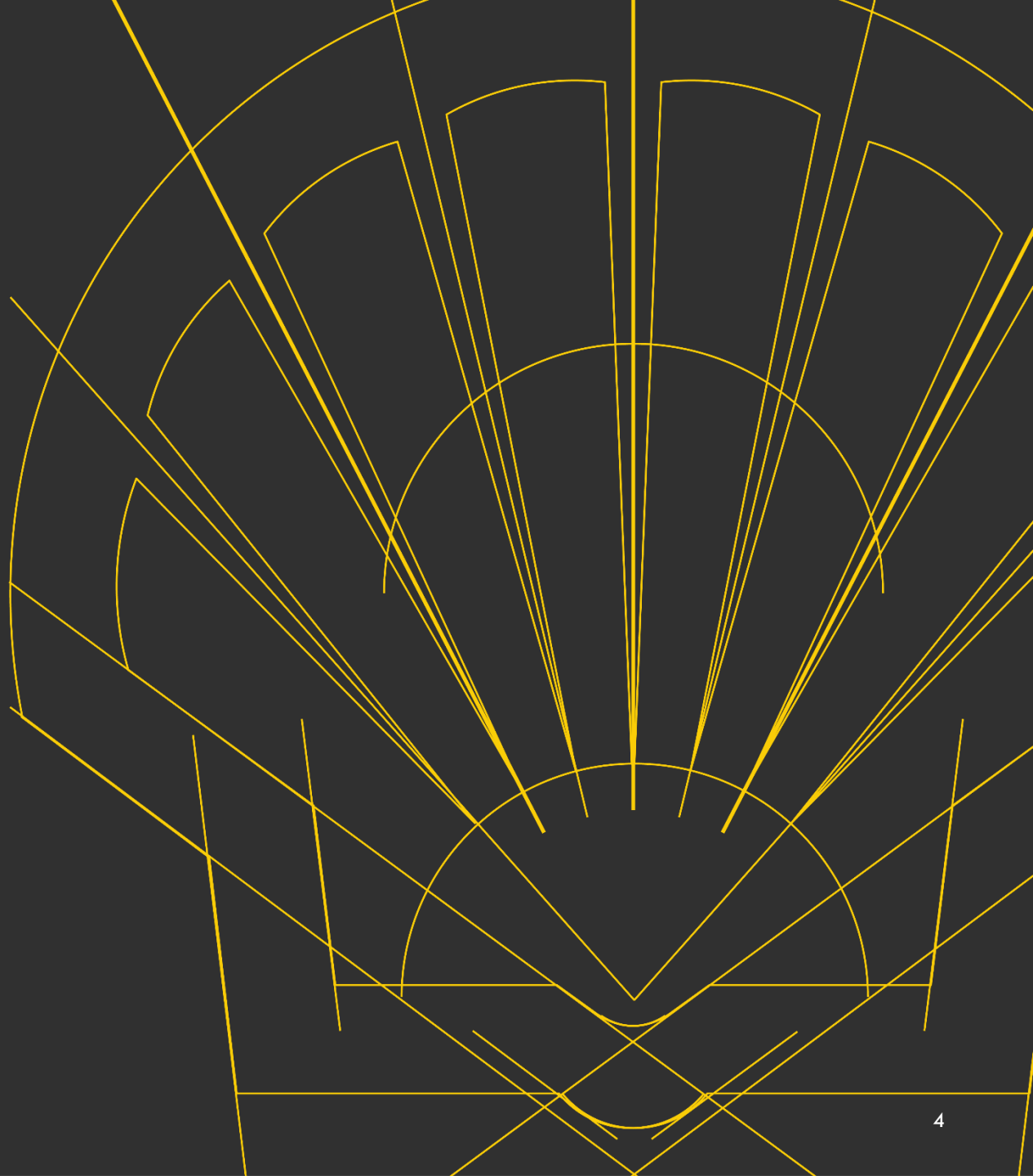
Anti-Trust Reminder

- Meeting participants are reminded that the parties are competitors in certain markets, and are subject to antitrust/competition laws
- The parties are committed to compliance with all applicable laws and regulations, including antitrust/competition laws
- Any discussions are for the purpose of the development of a system to wirelessly exchange safety-critical fueling data between hydrogen vehicles and dispensers and are subject to legal advice to ensure compliance with antitrust/competition laws
- Discussions which might be misconstrued as price fixing, customer or market allocation, attempts to alter the competitive marketplace, or boycott suppliers and customers are not allowed
- Discussions of competitively sensitive subjects such as an individual company's marketing strategies, supply and demand forecasts, open season bids, vendor specifics, business strategy, and customer information are not allowed
- If any meeting participant has any questions/concerns regarding these antitrust considerations with respect to the meeting, he/she will consult his/her counsel
- All meeting participants are encouraged to promptly object to any material, presentation, comment, or question that they do not believe is legally appropriate for the meeting

Overview

- Introduction to Shell TechWorks
- Hydrogen Fueling Today
- Problem Statement
- Solution Space
- Functional Safety in Communication
- Industry Activities

Introduction to Shell TechWorks



TECHWORKS

Shell's Boston-Based Innovation Center

ABOUT US

Shell's Projects & Technology group created TechWorks with a goal of establishing an innovation team with backgrounds outside of the energy industry to advance Shell's short-term product development capabilities.

We work with teams across all lines of Shell's business to identify high-value opportunities and provide solutions that deliver real, tangible value to the organization.

WHAT WE DO

SYSTEMS ENGINEERING

Understanding complex systems and data trends in order to identify and quantify high-value of opportunities.

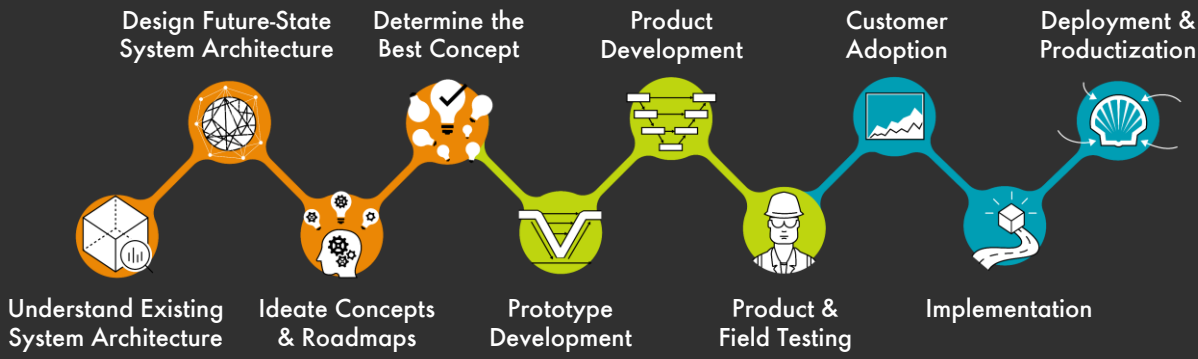
PRODUCT DEVELOPMENT

The development, testing, and verification processes that turn ideas into prototypes and functional products.

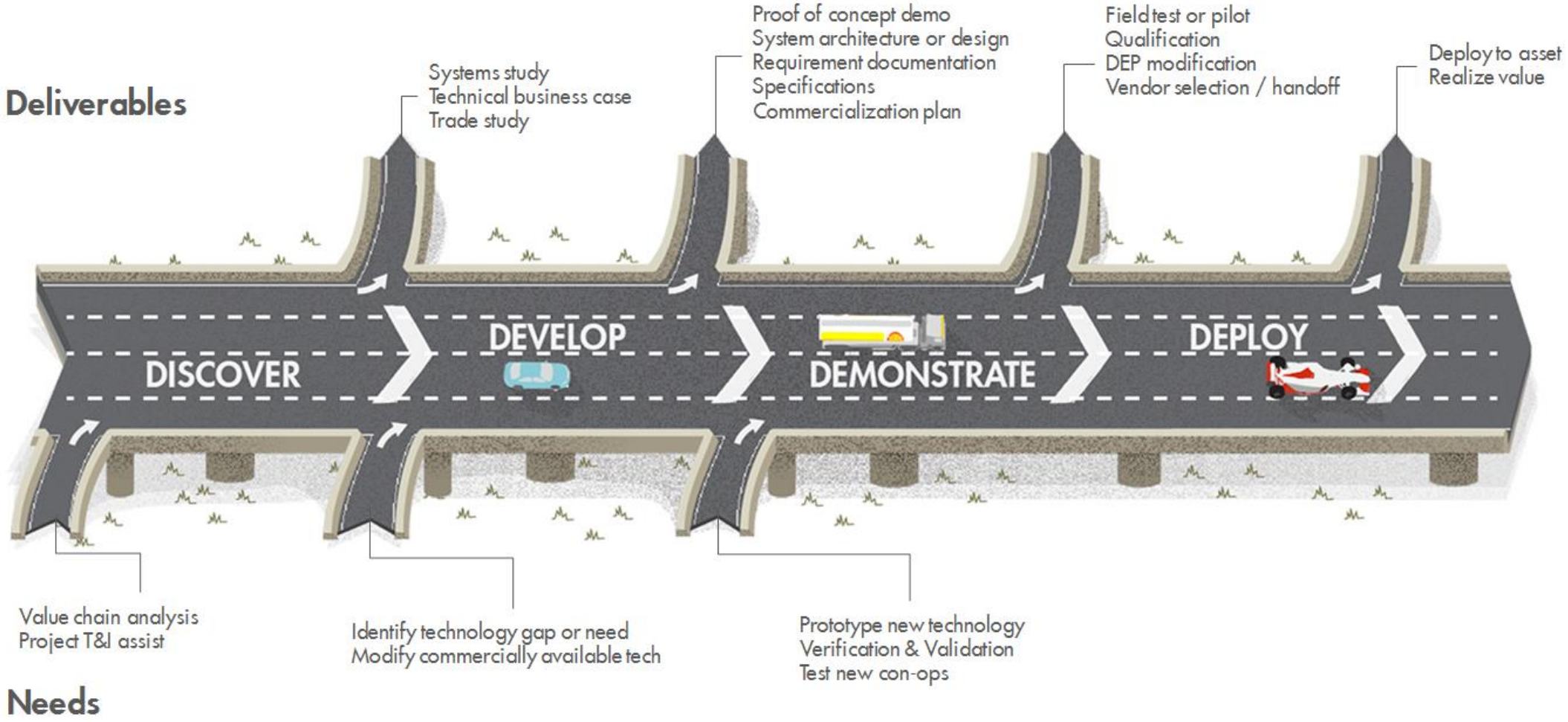
DEPLOYMENT & PRODUCTIZATION

Scaling solutions and guiding adoption into Shell's business through collaboration with internal and external partners.

OUR APPROACH



Working with TechWorks



Project Background

Colocation & Collaboration

Shell Hydrogen in the US was born out of a systems study at Shell TechWorks

Heavy-duty Fueling Times

Long fueling times for heavy duty vehicles were identified as challenge to Shells hydrogen strategy

Vehicle to Dispenser Data

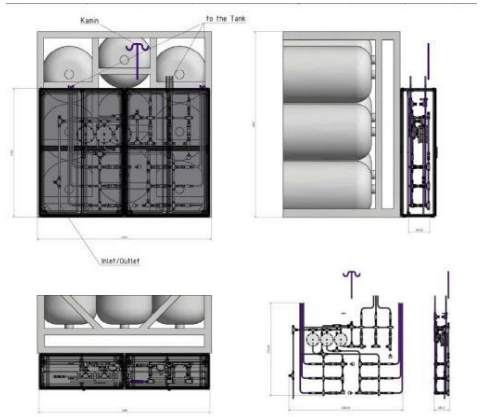
Bottleneck is communication of safety critical fueling data from vehicle to dispenser to be able to use an advanced fueling protocol

In-House Product Development

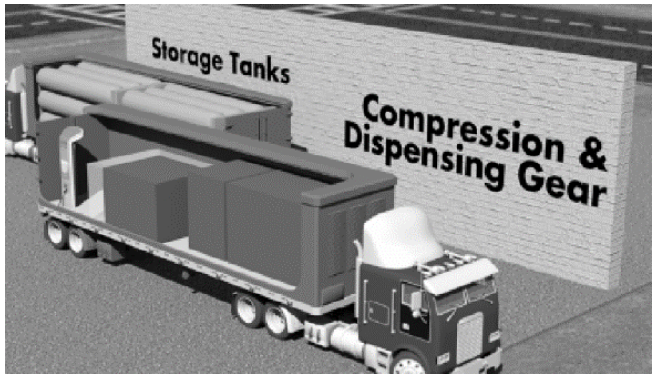
Shell TechWorks has competence in the area of electronics, communications and networking

Shell's H2 Activities (some of them)

Shell Hydrogen Power Dispenser



High-Capacity Storage



Mobile Refueler

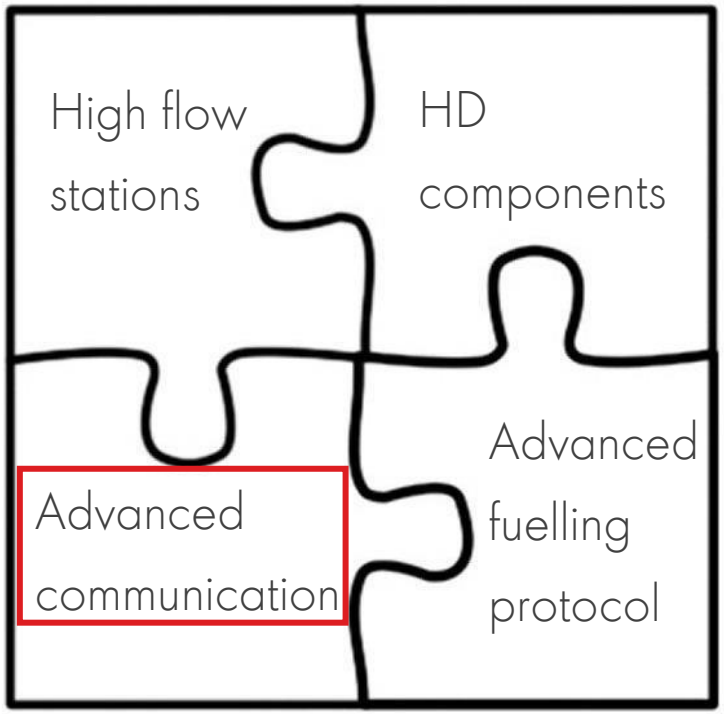
High-Capacity Transporter

Hydrogen for Heavy Duty: path to success

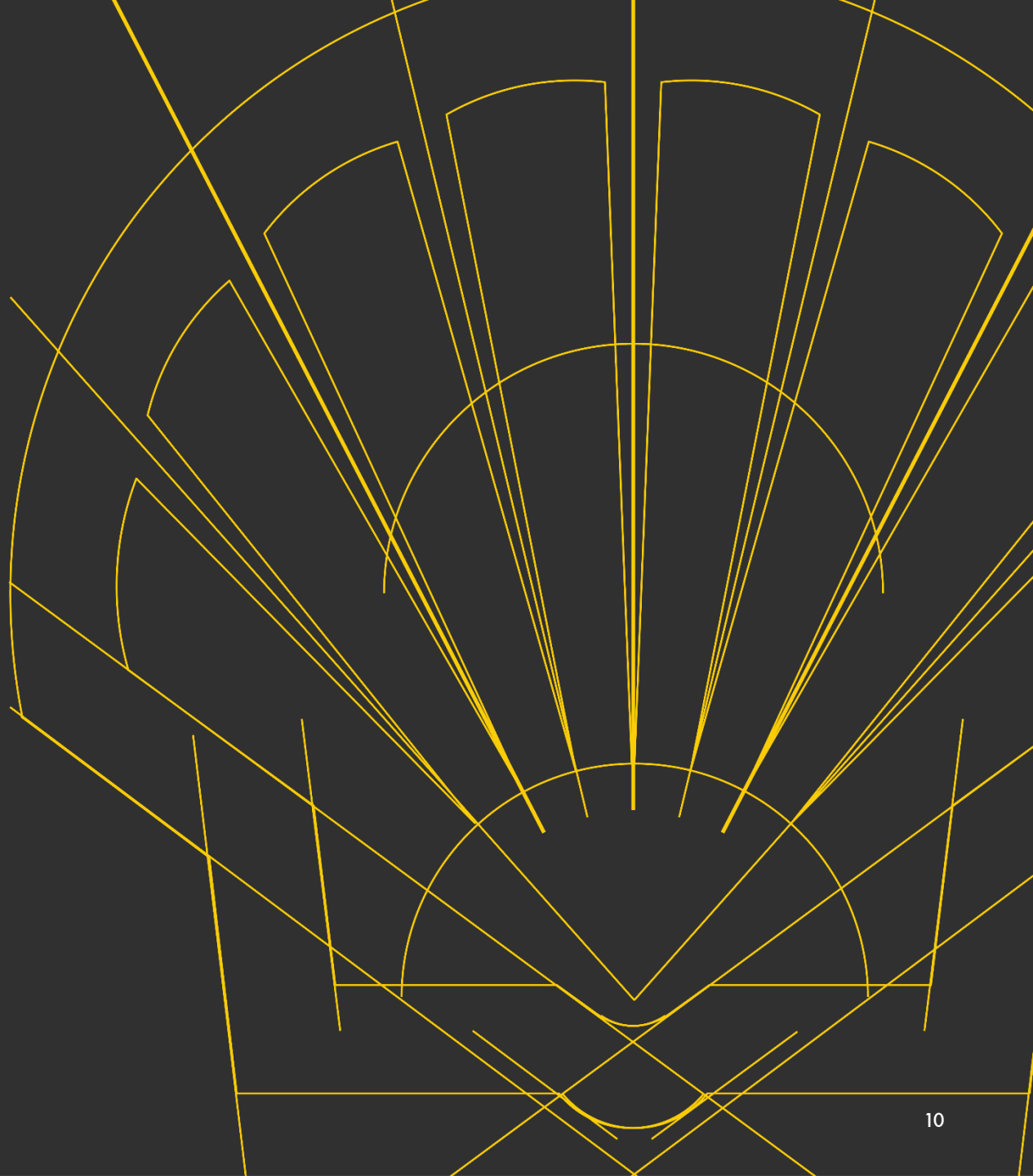
- The key to success in heavy-duty sector is parity with Diesel in:
  - Total Cost of Ownership
  - Range and Refueling speed → **80 kg of hydrogen filled in 10 min**

- This refueling performance is only achievable with these 4 elements
  - HD components => Hydrogen Heavy Duty Industry Group Consortium

  - High-flow stations
  - Advanced fueling protocol => PRHYDE Protocol for heavy-duty Hydrogen refuelling
  - Advanced communication => HyConnect

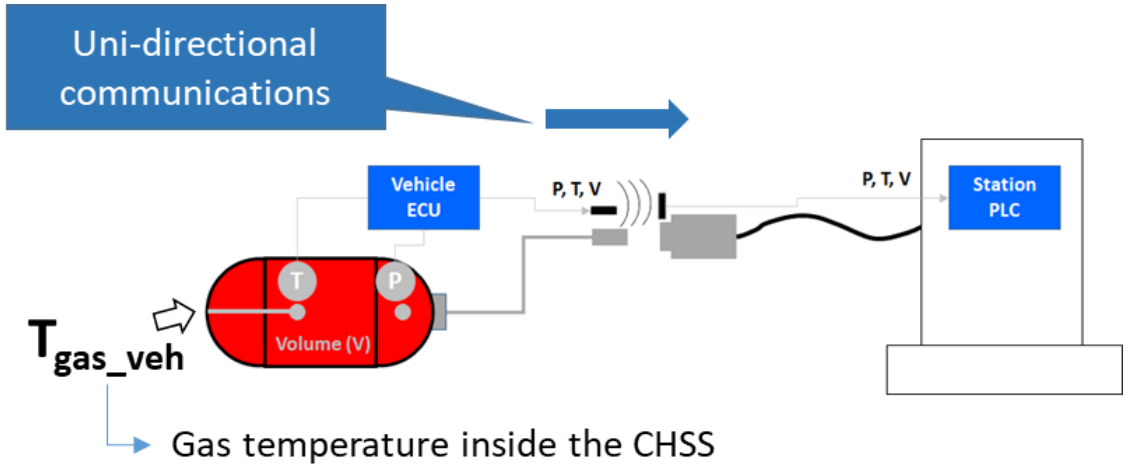


Status of Hydrogen Fueling Today



Fueling Protocol SAE J2601 (State-of-the-art)

SAE J2601:



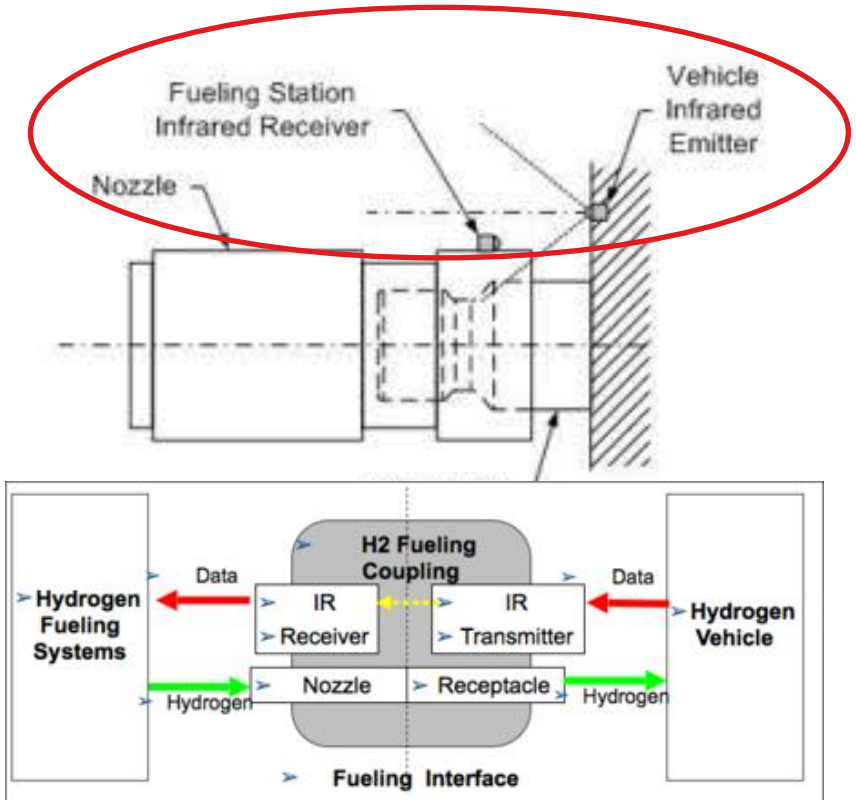
Graphics from Steve Mathison, NREL

- Tank of H2 vehicle heats up during fueling, mandates control of fill rate and pre-cooling of H2
- Design philosophy for J2601
  - Station assumes full responsibility
  - No exchange of safety critical fueling data
- Originally developed for passenger vehicles
- Dispenser measures initial tank pressure, tank volume, ambient temperature and fuel delivery temperature to calculate fill rate and final pressure
- Large safety margins, barely sufficient for passenger vehicles (fueling times 3-5 min)

Heavy duty:

- Fueling times >30 min if using J2601 (tank size 80 kg H2)
- Goal is <10 min, depending on tank size

Infrared Communication Vehicle/Dispenser

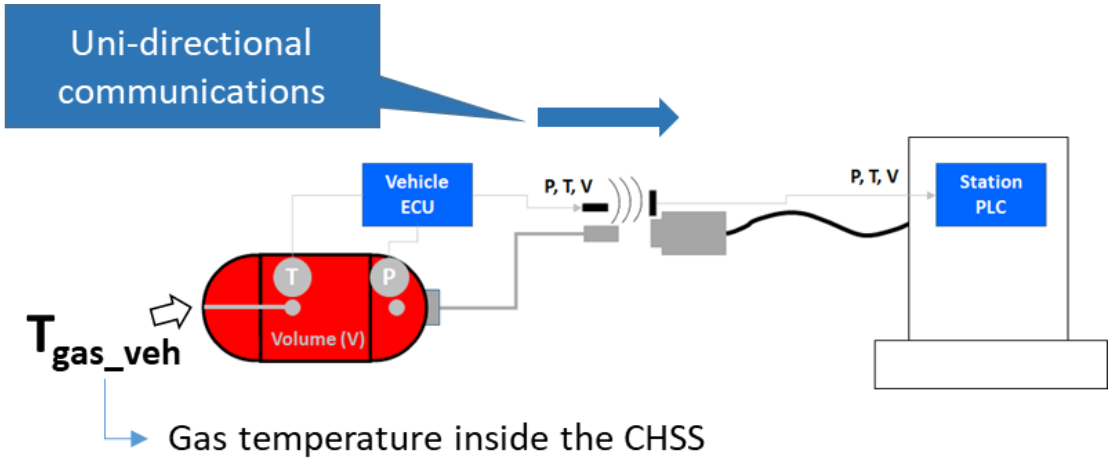


SAE J2799 specifies IR interface and data protocol

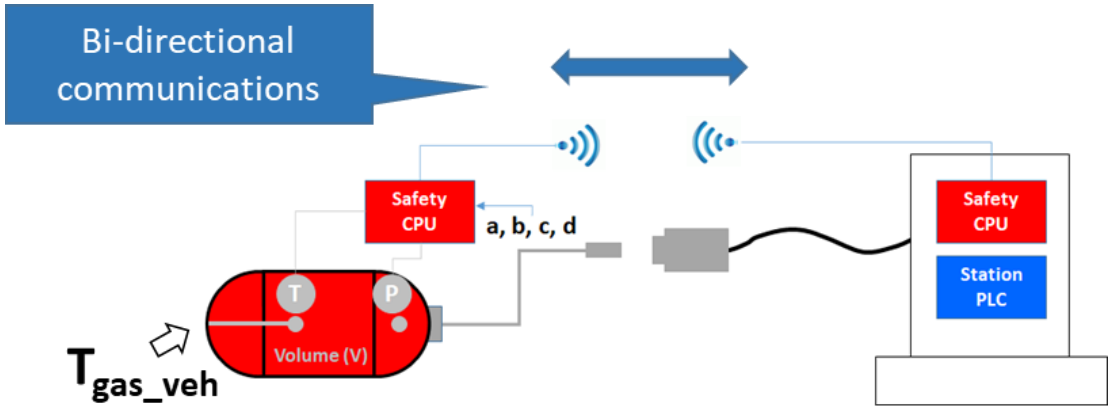
- Uni-directional communication only -> intrinsically not possible to communicate safety-critical data
- Communication activity
  - Start after nozzle inserted and start up routine has started
  - Continuously during fueling; transmit: p, T, fueling command
  - Use as long as dispenser receives data
  - Comms lost during fueling: abort or continue w/non-comms
- Communication only to improve state of charge (SOC)
  - BUT limited by calculated target pressure

Source: Weh, IRDI Systems, J2601/2799

Future: EU Project PRHYDE



Future:



- Different solutions are possible
  - Type 1 - Reduce safety margins (keep existing comms)
  - Type 2 - Communicate extended parameter set that characterizes tank(s)
  - Type 3 - Feedback control fueling (p, T transmitted continuously)
- The latter two assume availability of communication channel for safety-critical information
- Standardization of Prhyde fueling protocols is planned in ISO 19885-3

Graphics from Steve Mathison, NREL

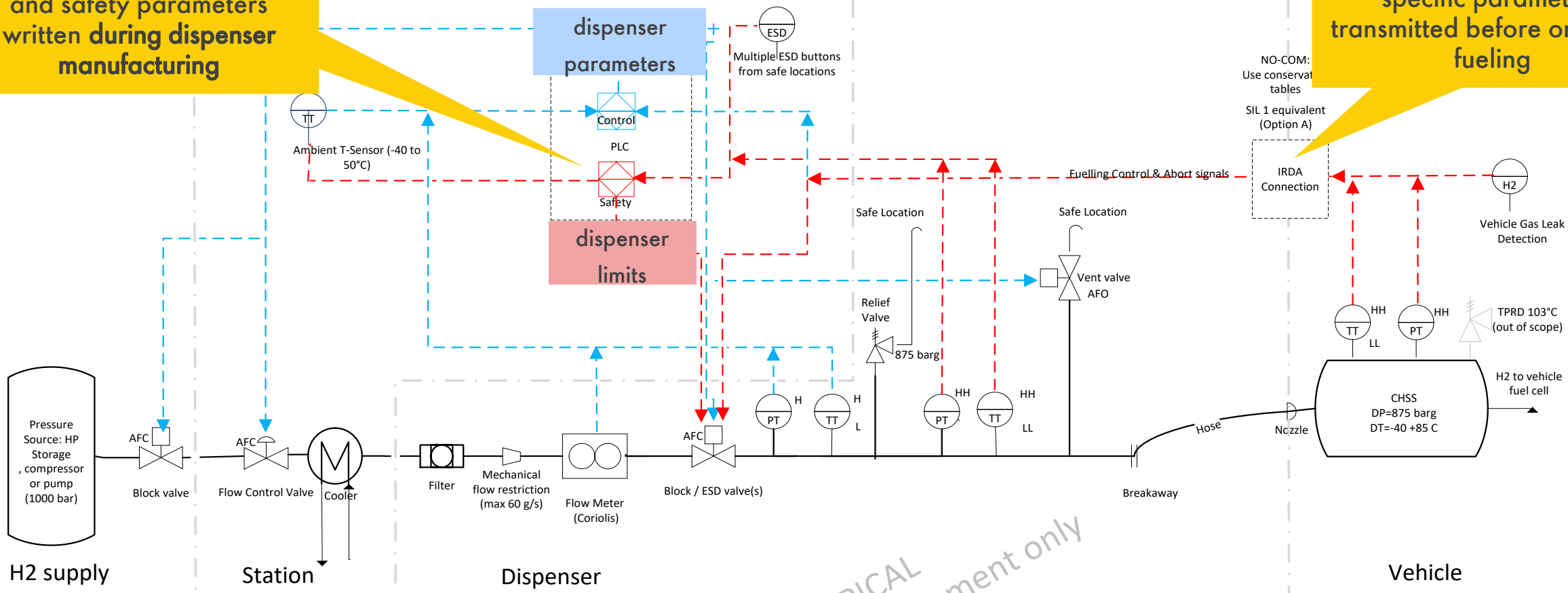
Future: Expanded Vehicle Fleet

Graphics from Steve Mathison, NREL

Safety today (J2601) – dispenser/station

all J2601 process control and safety parameters written **during dispenser manufacturing**

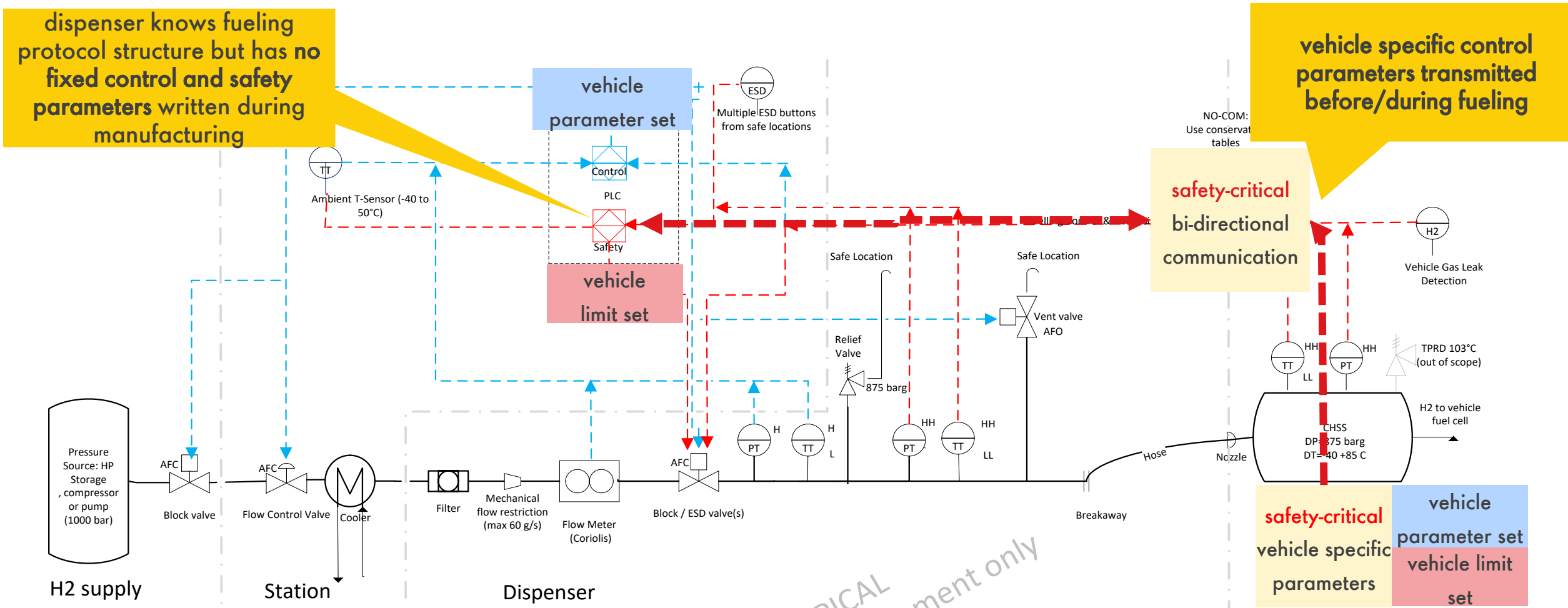
no safety-critical vehicle specific parameters transmitted before or during fueling



TYPICAL
r risk assessment only

Graphics from EIGA risk assessment

Safety in the future – dispenser/station



Graphics from EIGA risk assessment

Problem Statement

J2601/J2799:

- Large safety margins result in low fill rates and excessive pre-cooling/poor energy efficiency
- Uni-directional communication, does not allow transmission of safety-critical data
- IrDA unreliable, prone to error (sunlight, fogging)
- Easily damaged in field w/costly maintenance
- Vehicles with different tank configurations

Need:

- Reliable wireless communication of safety-critical fueling data between vehicle and dispenser
- Low-cost components
- Open standard(s), industry wide solution

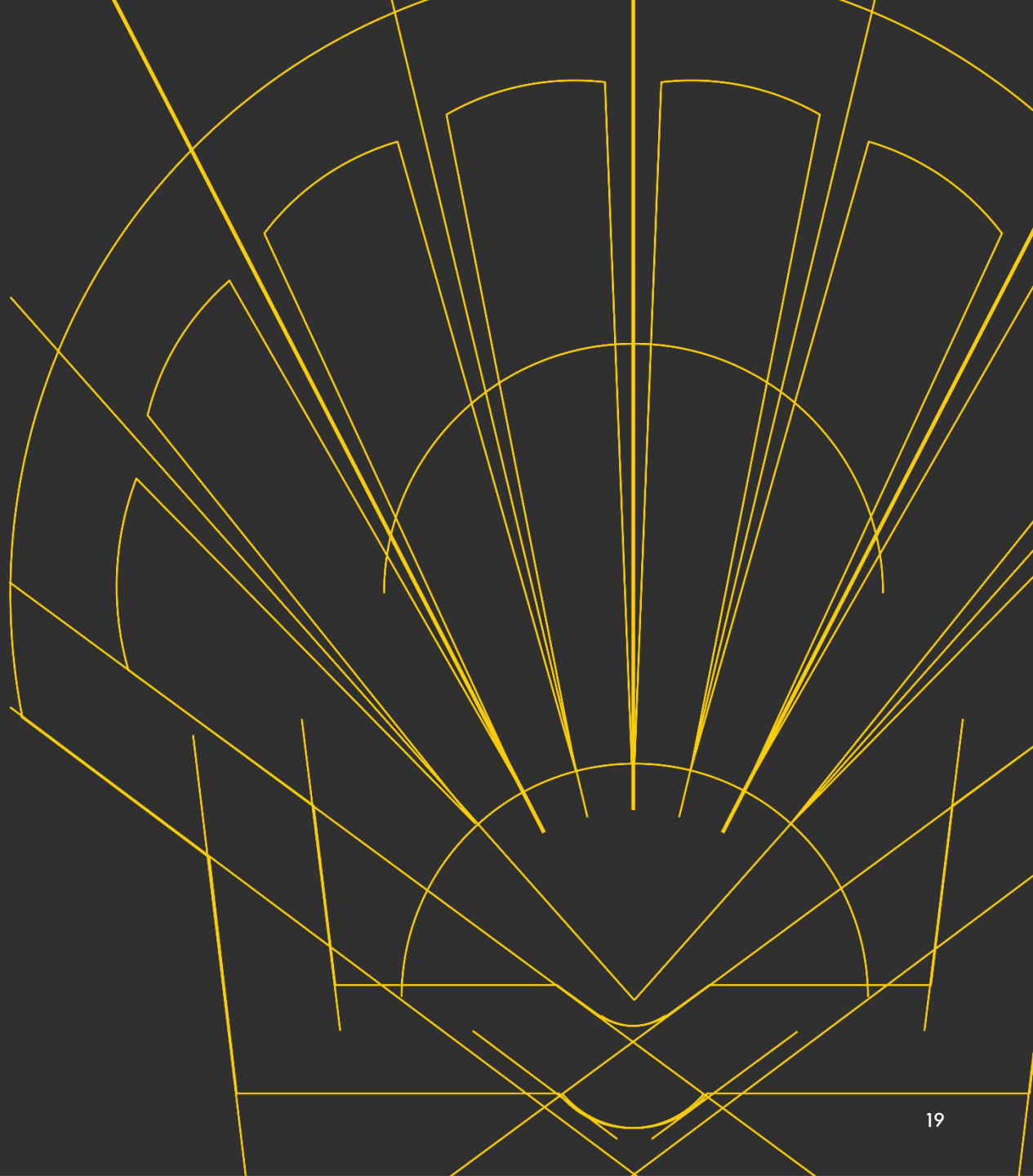
Enables:

- Advanced fueling protocols to decrease fueling times
- Improved energy management (pre-cooling)

Assumptions/Disclaimer

- **PRHYDE project has proposed framework for fueling protocols, some open questions remaining on**
  - Data to be transmitted
  - Vehicle/dispenser responsibility
  - Some others…
- **Assumption for the following:** Wireless communication of safety-critical data between vehicle and dispenser needed
  - Can be used to transmit static data (tank properties etc.) and dynamic data (temperature, pressure etc.)
  - Automatically bi-directional
- **Detailed implementation TBD**
  - Proposed implementations/examples in the following are to be viewed as a starting point and not "the" solution

Solution Space



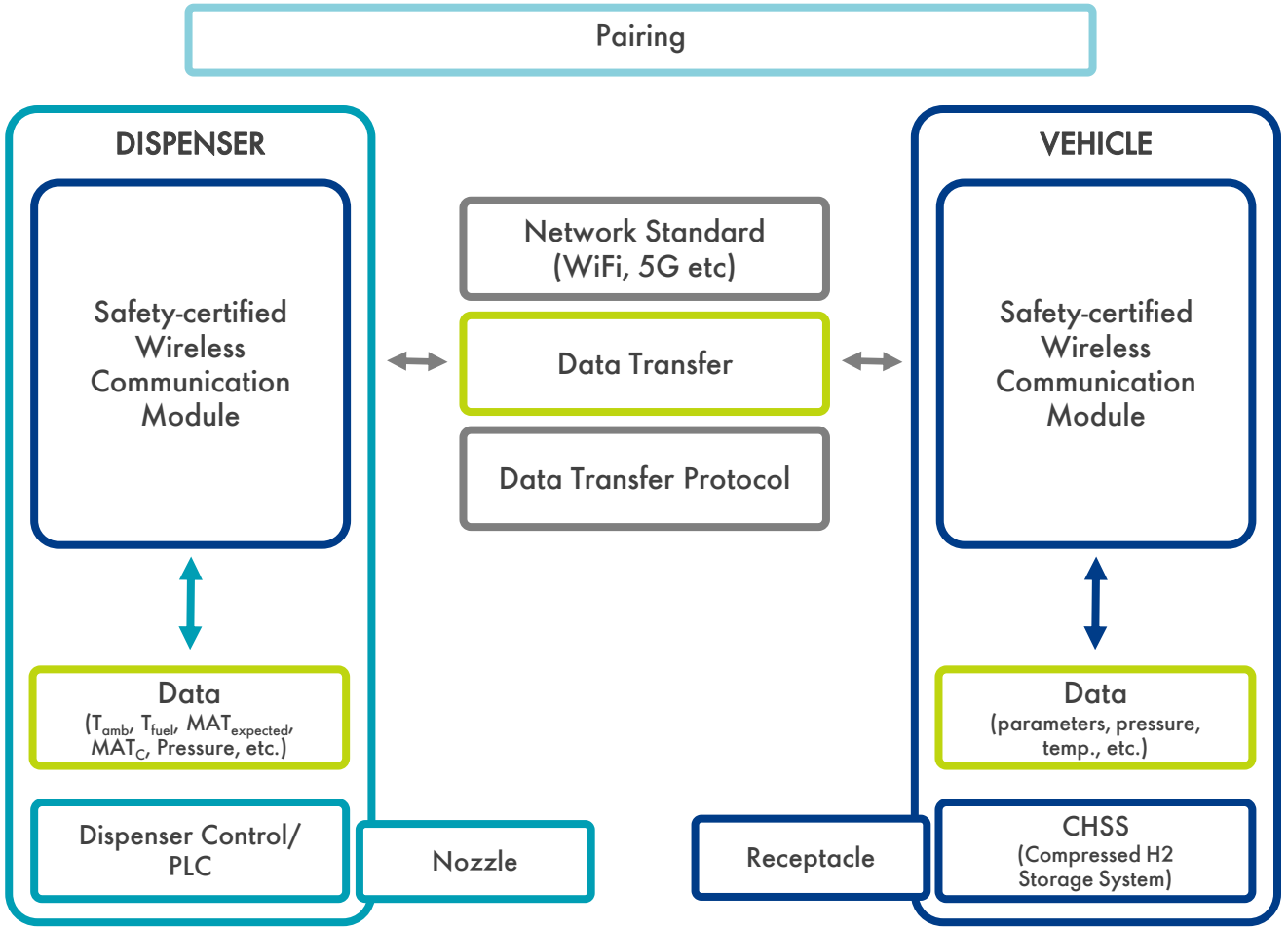
Proposed Approach

Key Features

- Bi-directional wireless communication modules in dispenser and vehicle
- Based on black channel communication IEC 61508
  - example: IEC 61784-3 defines safety protocol based on black channel comms
  - Vehicle/dispenser need safety-certified modules
  - Low cost, non-safety-certified network hardware beyond safety-certified modules

Needs

- Vehicle to dispenser pairing
- Trusted relationship between vehicle and dispenser



Sequence of events

fueling

- pairing
  - read vehicle identifying information (e. g. via NFC)
  - establish network connection between vehicle and dispenser (e. g. via Wi-Fi)
- authenticate vehicle and dispenser
- encrypt communication channel
- exchange fueling data (black channel)
  - static data before H2 flow starts
  - dynamic data (continuously) while H2 is flowing

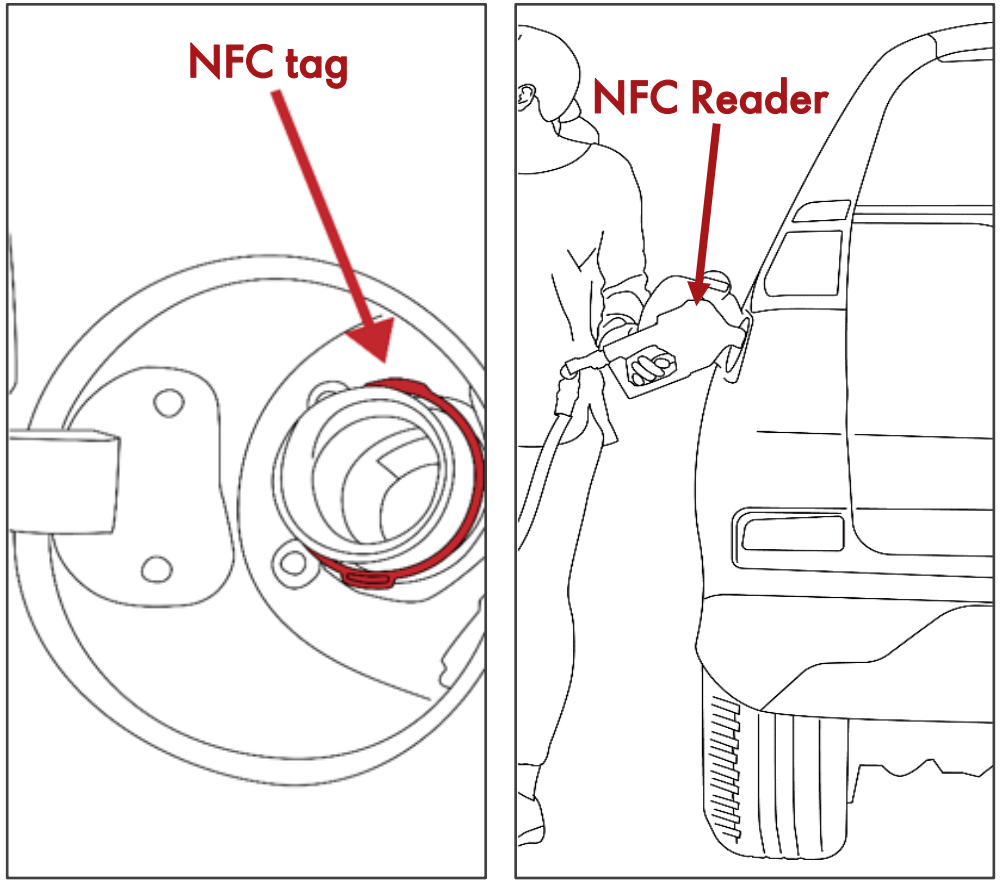
→ first time fueling protocol data gets transmitted (i. e. Prhyde)

production

- write **safety-critical** data to vehicle: static fueling data (look-up tables, parameters), certificate(s) for identity
- write **safety-critical** data to dispenser: certificate(s) for identity

Vehicle to Dispenser Pairing

- Vehicle enters station forecourt and stops in front of dispenser, how to establish 1:1 network connection (pairing)?
- One possible solution is based on NFC to establish pairing
- **Example**:
  - NFC tag on vehicle fuel receptacle
  - NFC reader on fuel nozzle
  - Once the two come into sufficient proximity the NFC reader reads vehicle identifying information from the NFC tag
  - The dispenser uses the vehicle identifying information to establish a network connection with the vehicle
- Alternatives: bi-directional NFC communication vehicle/dispenser, use RFID instead of NFC, etc.



Establishing Trust

Who are you?

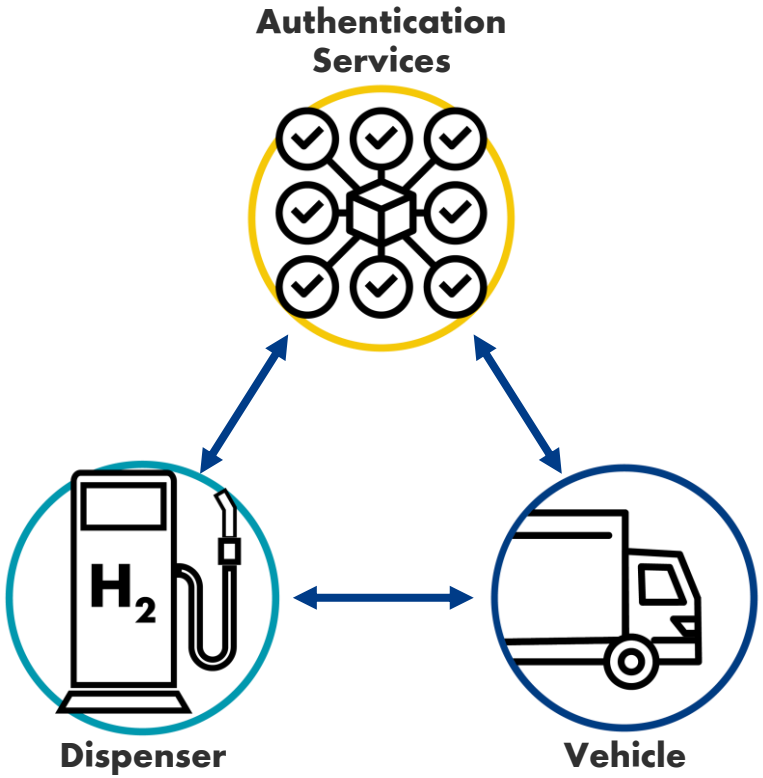
- How does dispenser know the vehicle is what it advertises itself to be and vice versa?
- Potential HSSE incident if vehicle reports as something it's not

Identity Management/Authentication

- Use industry standard identity and access management (IAM) paradigm
- After vehicle and dispenser have paired, identity certificates are exchanged
- Certificates are validated by a trusted party

Encryption

- To securely communicate across insecure channels



Existing vehicle wireless communication

Bluetooth

- Hands-free music streaming, rear-seat entertainment
- Tire pressure monitoring (TPMS) and Battery Management
- Secure communication for keyless entry

Wi-Fi

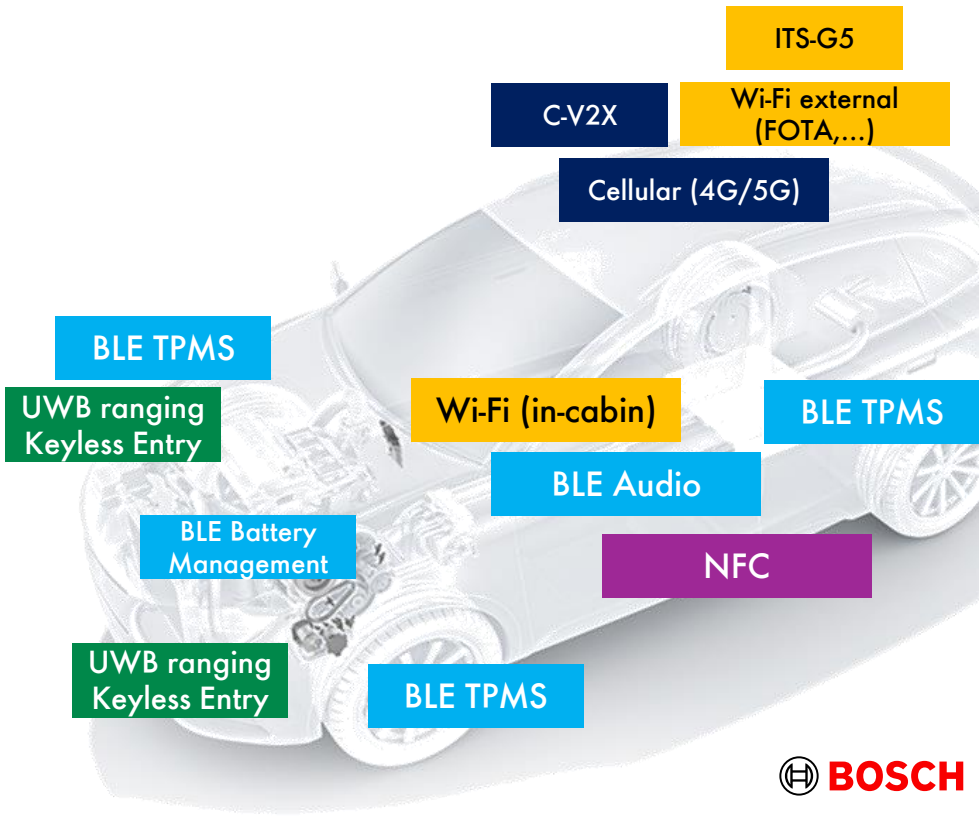
- Infotainment for in-cabin, auxiliary devices (e.g. cameras)
- Firmware over the air (FOTA) and EV wireless charging control
- Automated valet parking (functionally safe)
- ITS-G5: Hazard warnings (secure communication)

UWB (ultra wide band): Secure ranging for keyless entry

NFC: Secure communication for Vehicle access

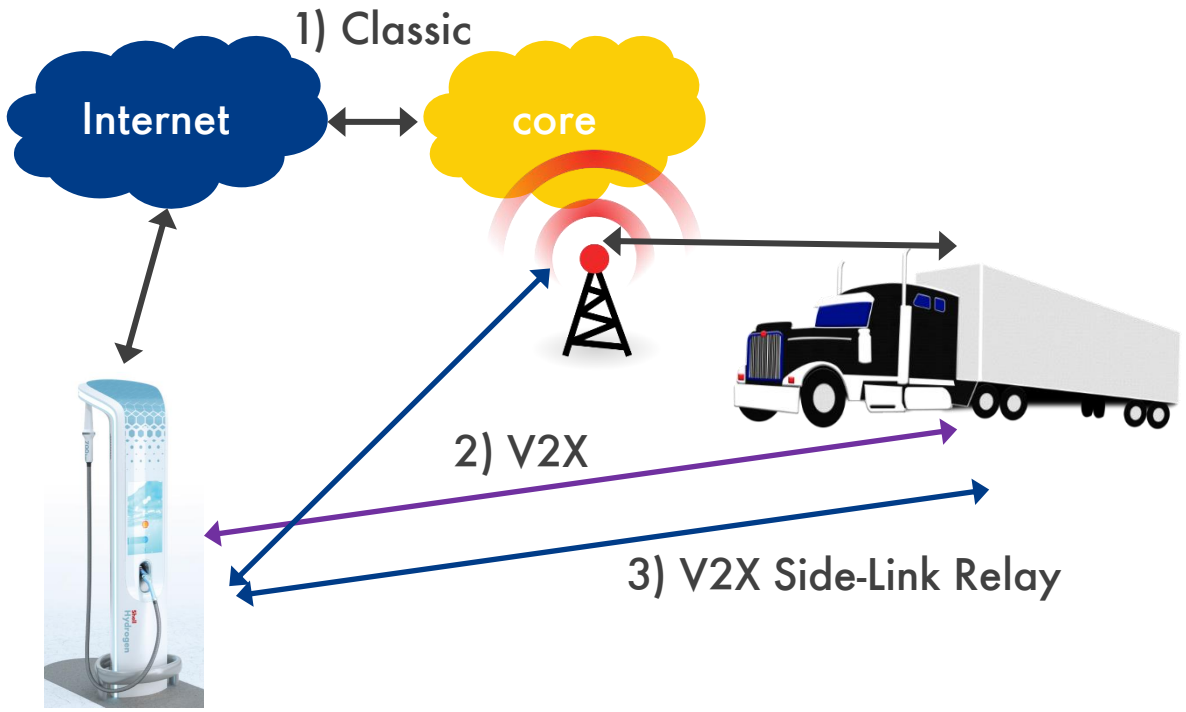
Cellular

- eCall, infotainment, network-based services
- C-V2X : Tele-operated driving (functionally safe)



BOSCH

Cellular: 4G and 5G (and beyond)



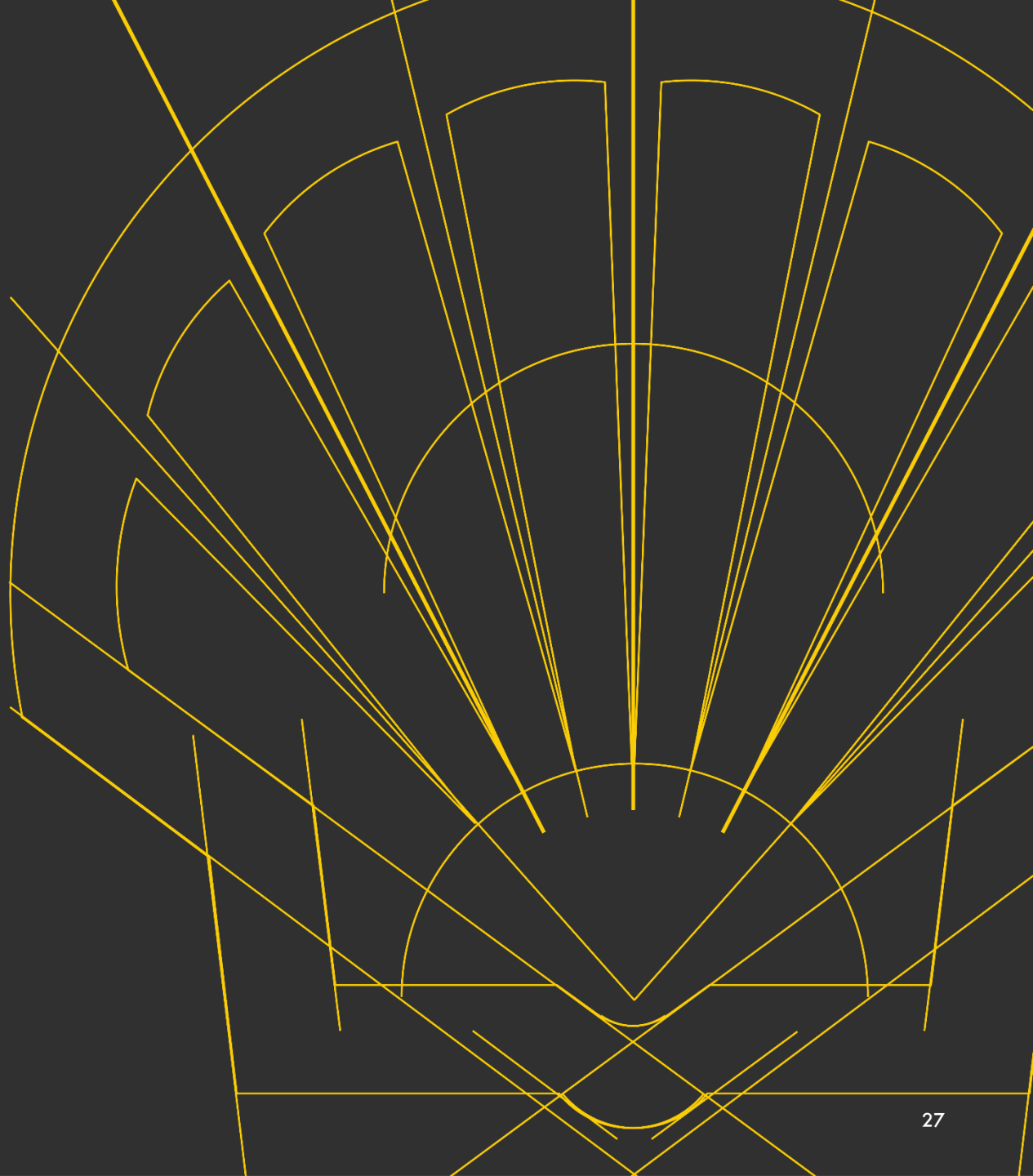
- 3GPP Release 15: rolled-out, available
- Rel. 16 first modules available
- Rel. 17: specified until 6/2022, modules by end of 2022

- 1) Classic 1G…5G system (via cellular network)
  - Ultra-reliable low-latency communication: latency approx. 5 ms (Rel. 17)
  - device-to-device not supported yet (Rel. 17+)
- 2) V2X allows direct communication without cell tower (resource allocation mode 4) and low-latency communication (Rel. 14: 4G-V2X)
- 3) V2X Side-Link: One side as relay to cell tower (Rel. 17)

Once secure communication is established…

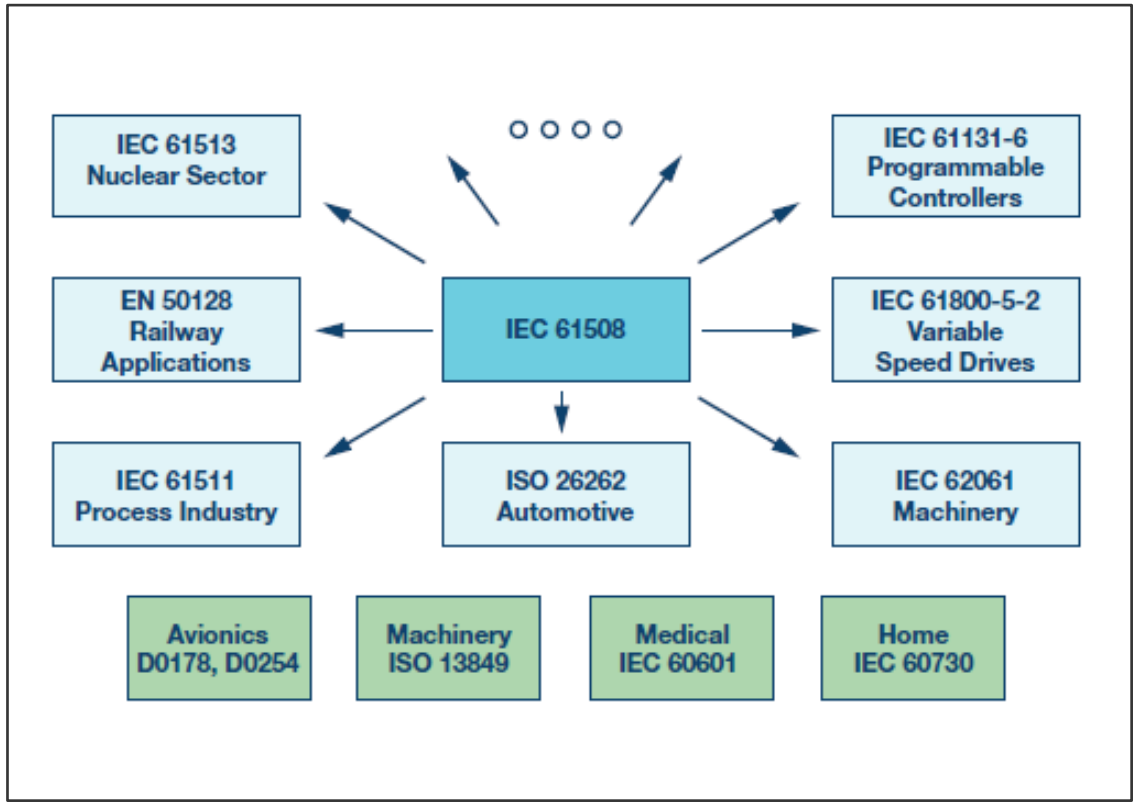
- Fueling data can be exchanged
- Additional services can be offered to the customer
  - Automatic use of loyalty programs (fuel rewards, fleet cards etc.), product offerings etc.
  - Fleet management (status/maintenance/fueling/payment data, remote access to vehicle data, etc.)
- Fully automated payment can be executed
  - The customer (pre)registers payment information
  - Payment information is obtained by the dispenser via the secure communication link, resulting in a truly frictionless transaction (i. e. user does not have to enter any payment information)
  - Multi-factor authentication can be used where the car itself can be used as one factor (knowledge = something only the user knows, possession = something only the user has and inherence = something only the user is)
- Logging of fueling data/operation, vehicle/tank properties can be performed for future analysis/optimization/safety improvement etc.
- …many more…

Functional Safety in Communication



Functional Safety (and Security) in Communication

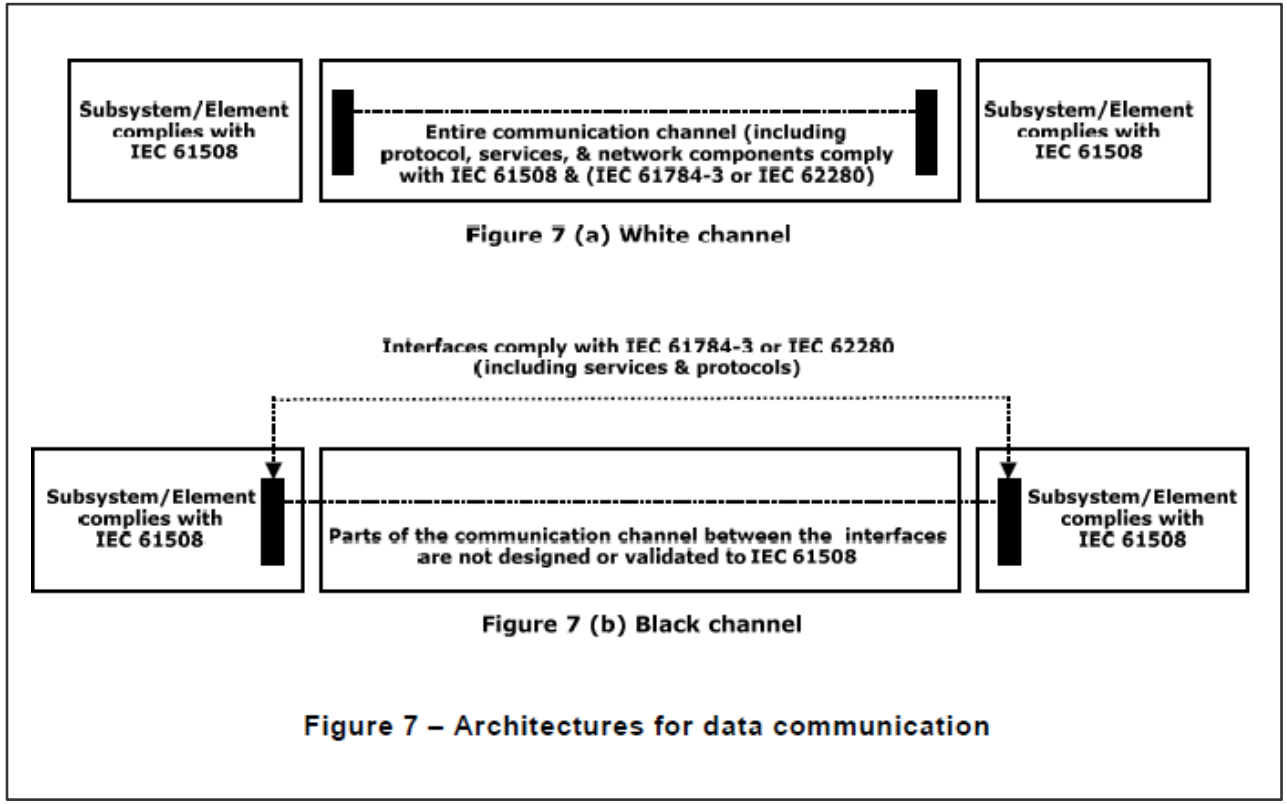
- Security = prevent harm due to intentional actions (i. e. hacking)
- Safety = prevent harm due to unintentional actions (i. e. random packet loss)
- There is no safety without security
- Dispenser Side
  - Functional safety IEC 61508
  - Safety-critical communication IEC 61784-3 (fieldbus systems)
  - System security IEC 62443
- Vehicle Side:
  - Safety ISO 26262 (adaption of 61508 for automotive)
  - Security ISO 21434 (draft), SAE J3061 (non-binding), ISO 15504 (SPICE), ISO 2700x (general)



Graphics from Analog Devices

Black Channel vs. White Channel Communication

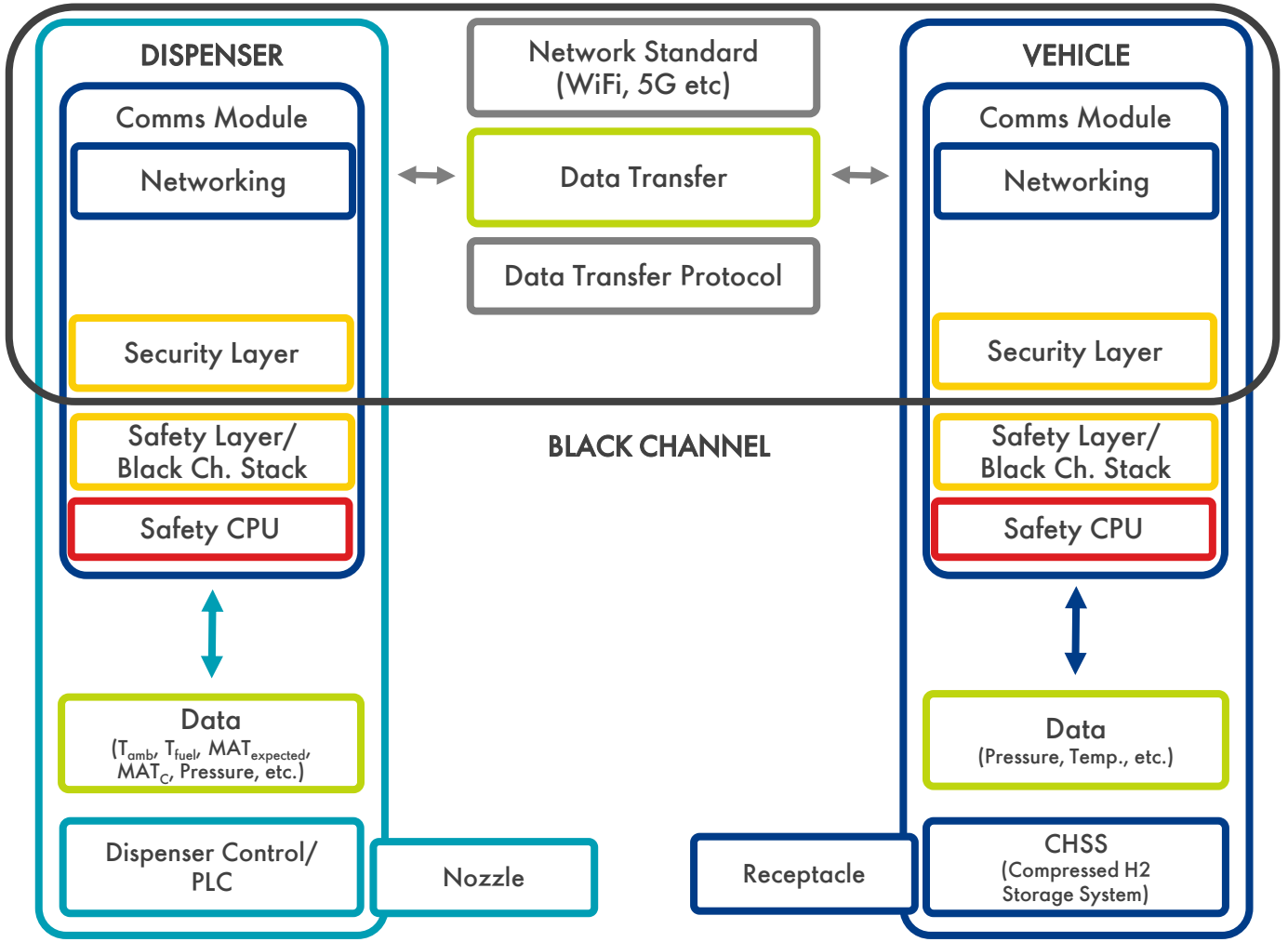
- White channel
  - entire communication chain of all elements is safety certified
- Black channel
  - only the two end elements of a communication channel are safety certified
  - all other components are standard (non-safety certified)
  - well known and established method in communications design



Graphics from IEC 61508

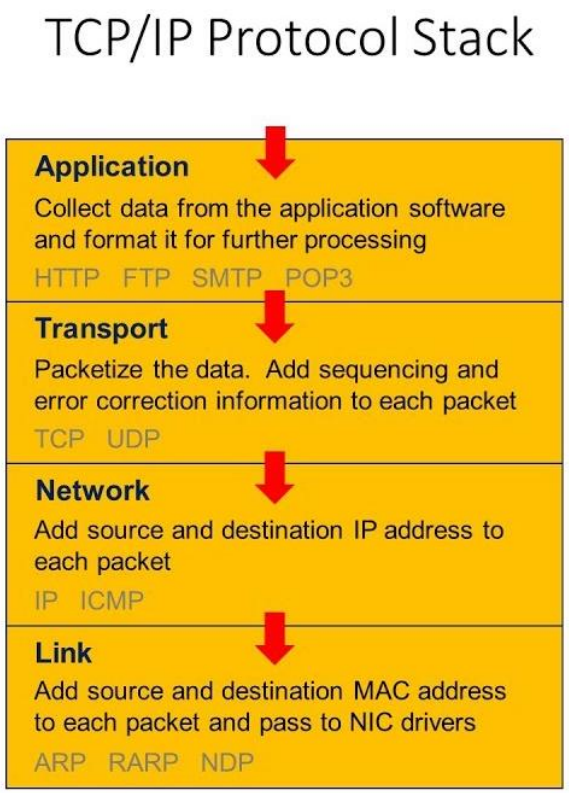
Black Channel Implementation - Hardware and Software

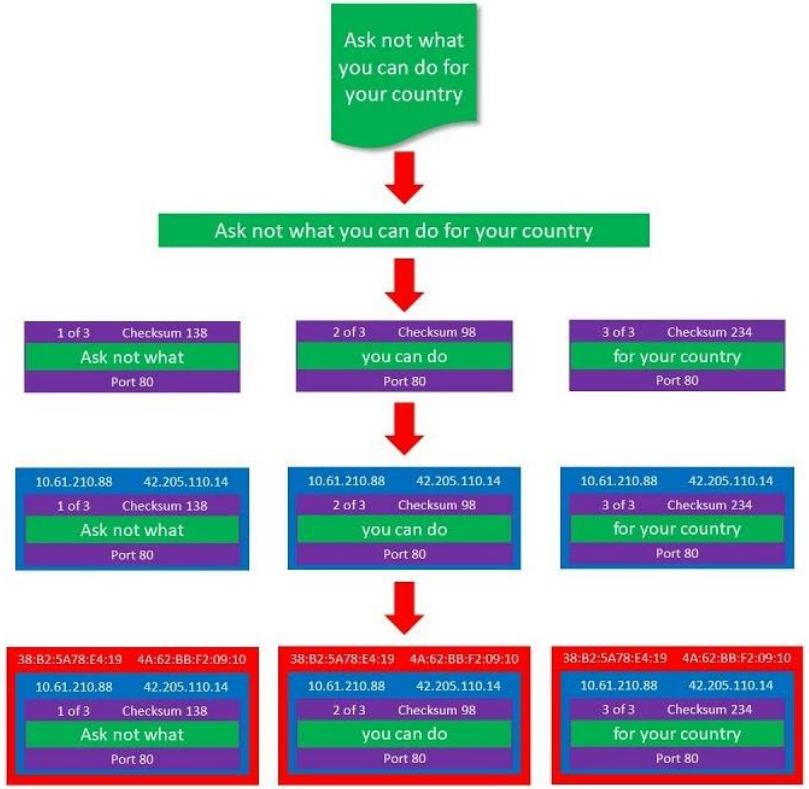
- Hardware
  - requires safety CPU
  - requires safety I/O to interface with PLC, sensors, bus systems
- Software
  - black channel stack running on safety CPU
- Networking
  - hardware can be standard, non-safety certified



Black channel – packets and encapsulation

- network communication: all data is transferred in packets
- data goes through different layers (OSI model, TCP/IP model etc.)
- safety-critical data is encapsulated into a safety packet by the black channel stack (safety-certified software running on safety CPU)
- safety packet is then handed over to standard, non-safety-critical software for packetization
- non-safety-certified hardware/software is unaware that safety-critical data is transmitted





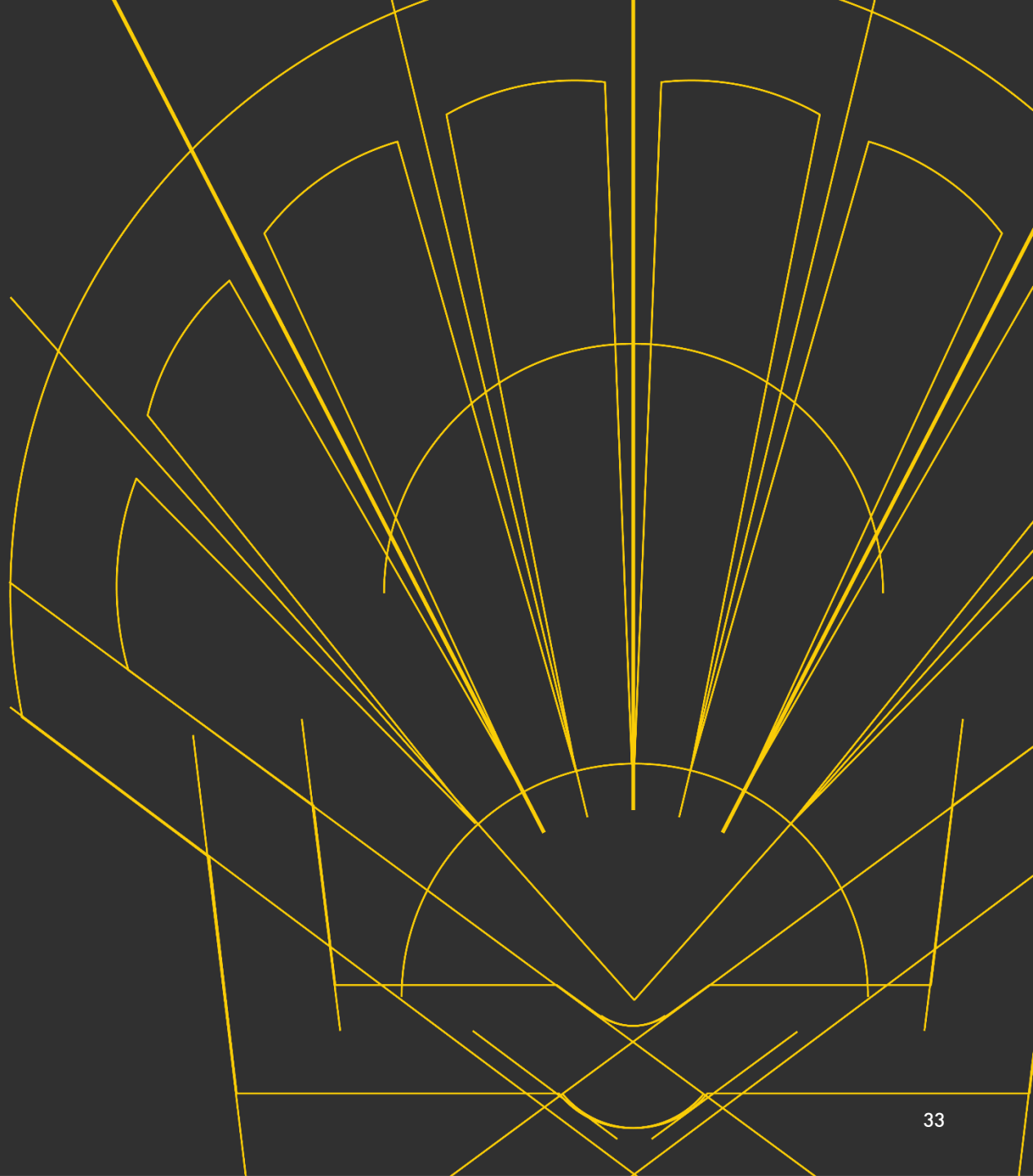
Black Channel Communication Safety Measures

- Must protect from various network errors
- IEC 61784-3 table1 provides a visual summary of communication error vs. safety measures
  - Corruption
  - Unintended repetition
  - Incorrect sequence
  - Loss
  - Unacceptable delay
  - Insertion
  - Masquerade
  - Addressing

Table 1 – Overview of the effectiveness of the various measures on the possible errors

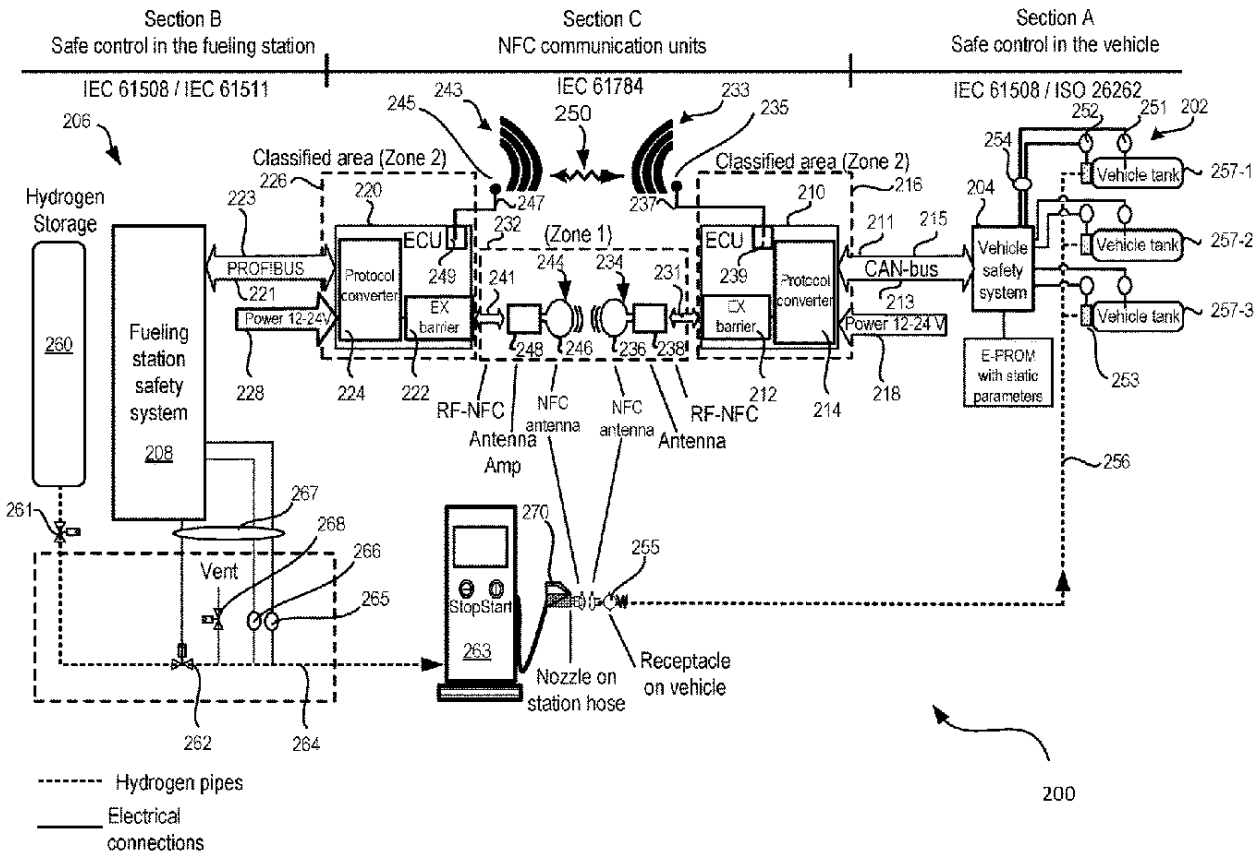
Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption (see 5.3.2)					X	X	Only for serial bus[d]	
Unintended repetition (see 5.3.3)	X	X					X	
Incorrect sequence (see 5.3.4)	X	X					X	
Loss (see 5.3.5)	X				X		X	
Unacceptable delay (see 5.3.6)		X	X [c]					
Insertion (see 5.3.7)	X			X [a,b]	X [a]		X	
Masquerade (see 5.3.8)				X [a]	X [a]			X
Addressing (see 5.3.9)				X				
NOTE Table adapted from IEC 62280-2 and [25].								

Industry Activities



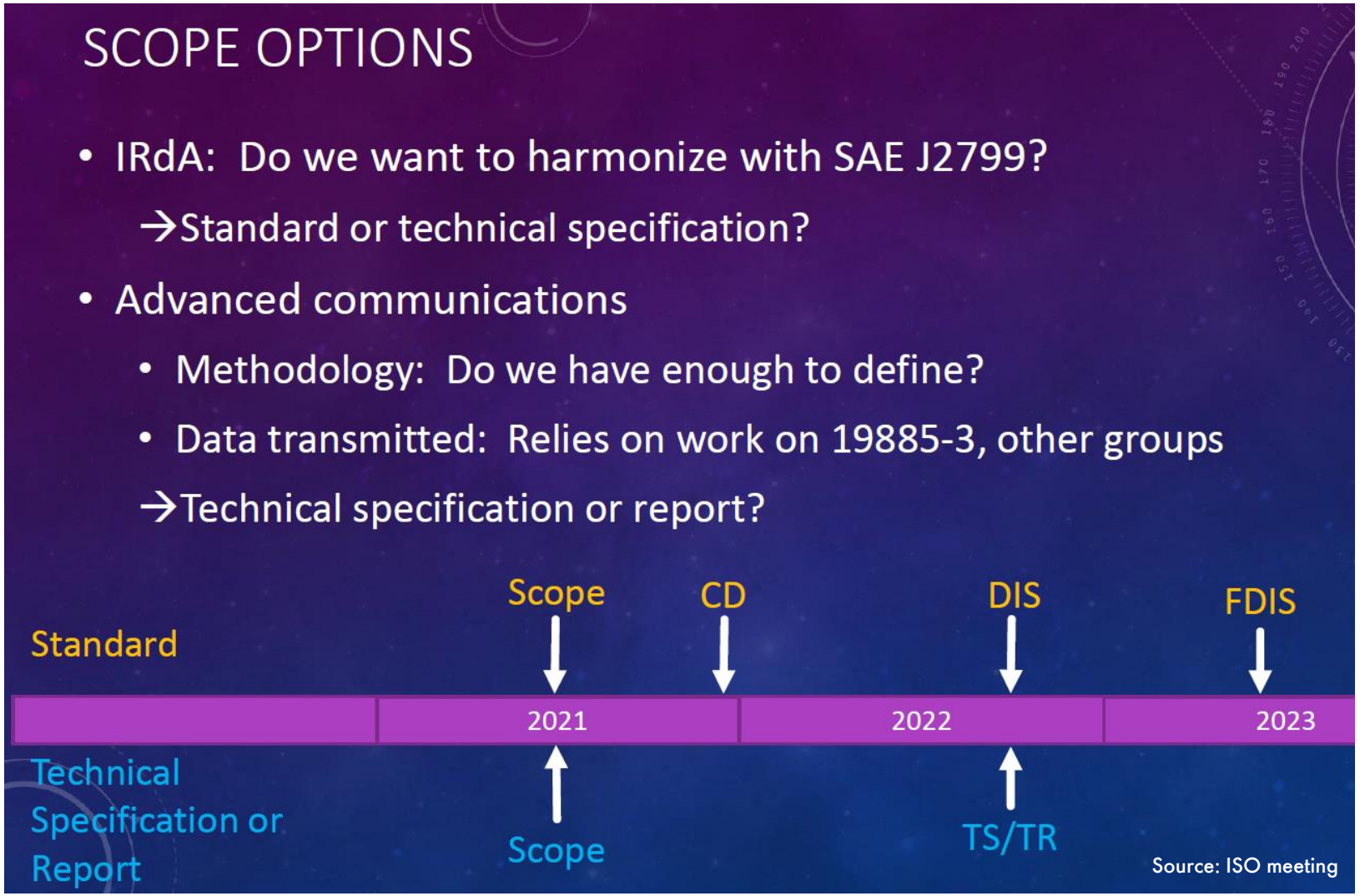
Patents

- US Patent: 10,800,281 "Communications Systems and Methods for Hydrogen Fueling and Electric Charging" (Priority Date: Feb. 18, 2019)
- Inventors: Nikola, NEL, Hoerbiger
- Concept: NFC + V2X bi-directional communications between vehicle and fueling station
- Nikola will offer the patent royalty-free to the HyConnect consortium and ISO/TC 197 to further develop and standardize the technology
- Nikola will participate in the preparation of technical papers for the dissemination to the public domain of any improvements in the technology to ensure standardization is not inhibited.

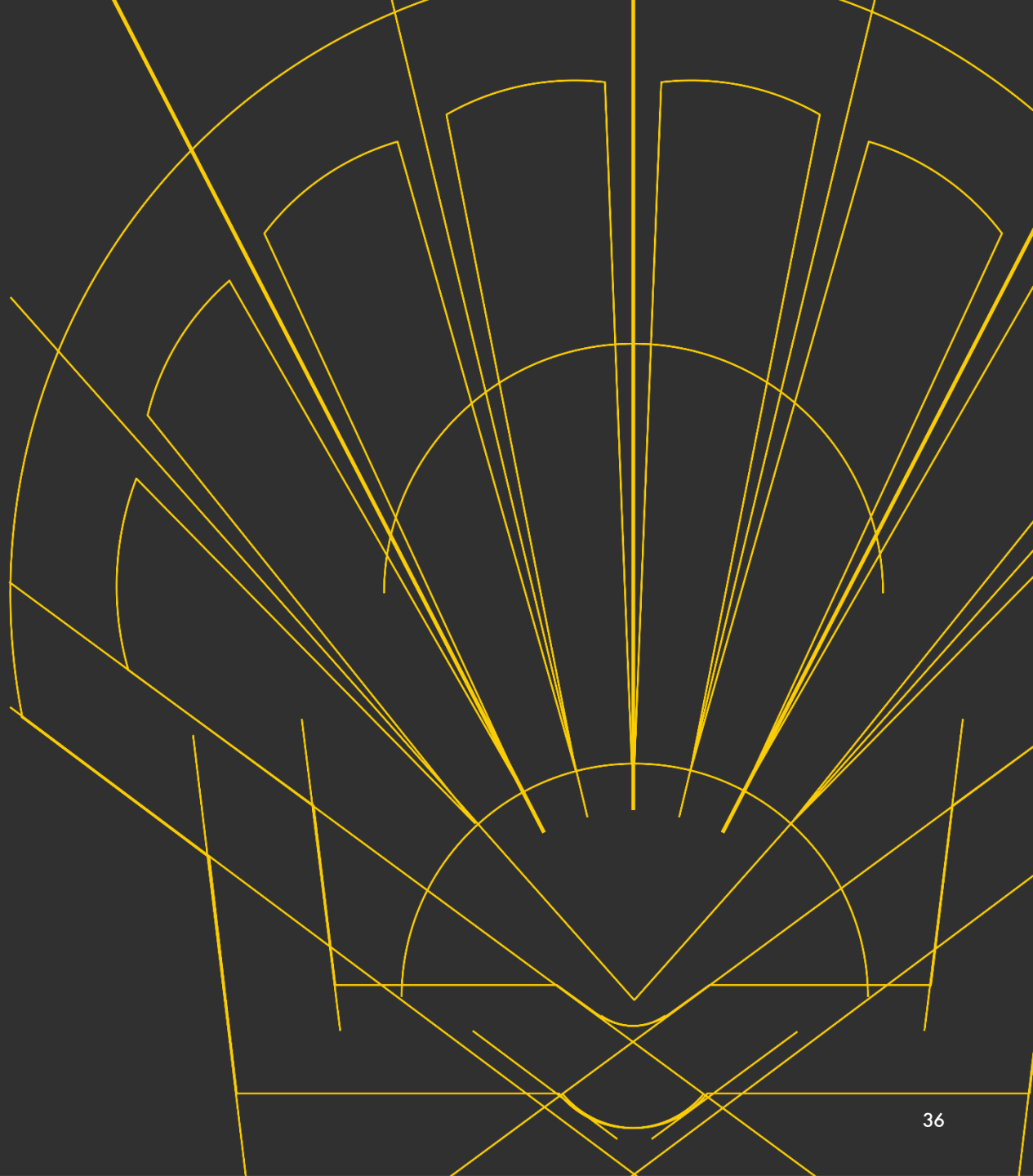


Standardization activities

- ISO has started activities to standardize fueling protocol(s) and vehicle/dispenser communication
  - TC 197/WG24
  - ISO 19885-1 – fueling protocols in general
  - ISO 19885-2 – wireless communication
    - ambitious timeline
    - next meeting ISO 19885-2 August 9/10, 2021
  - ISO 19885-3 – heavy duty fueling protocols (Prhyde)

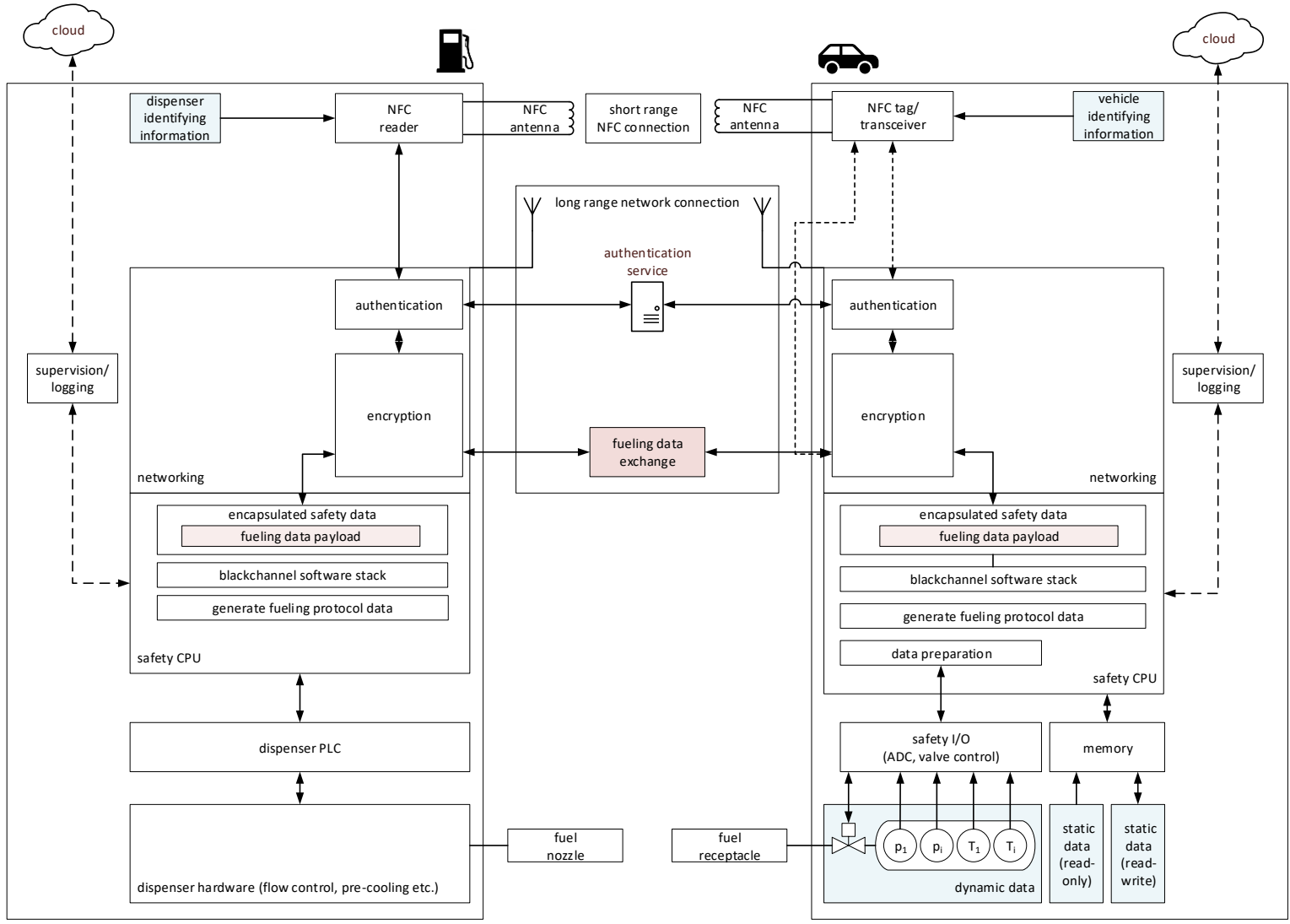


System and Interfaces

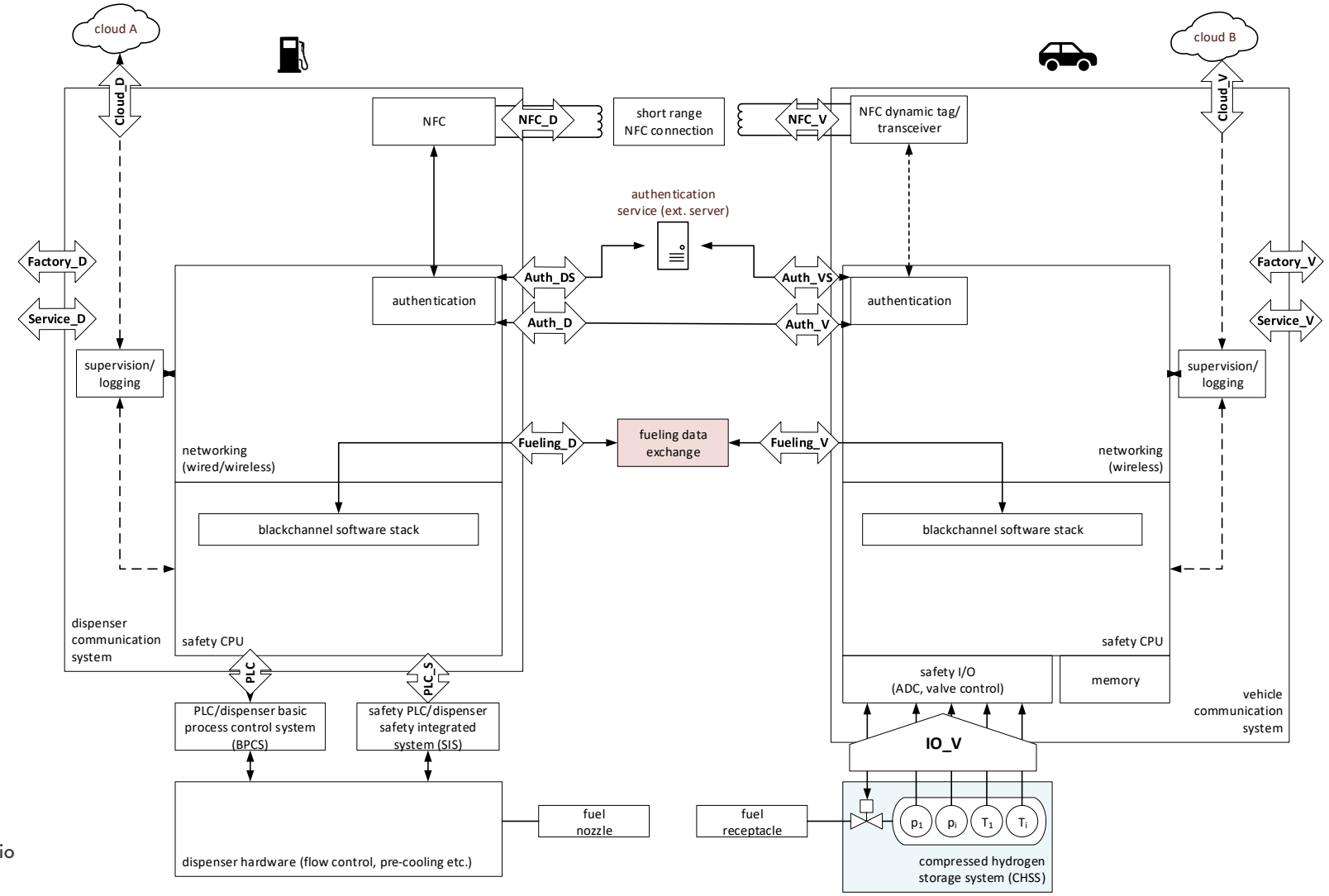


System Overview – More Details

- different for each vehicle/dispenser
- depends on vehicle EE-architecture and dispenser PLC configuration
- configuration will also depend on chosen Prhyde fueling protocol method (especially sensors)

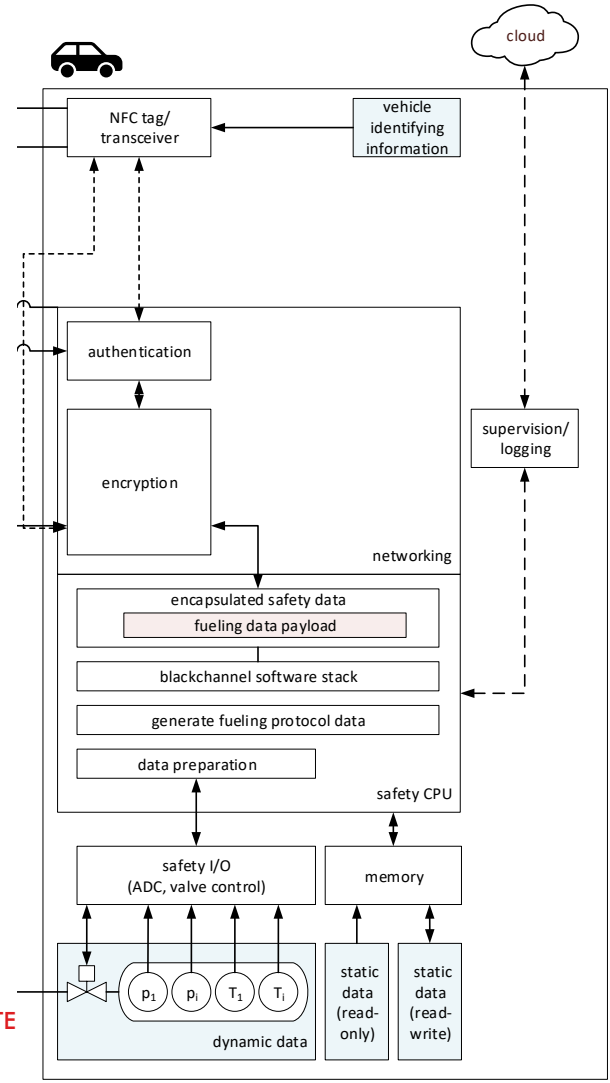


Interfaces Diagram



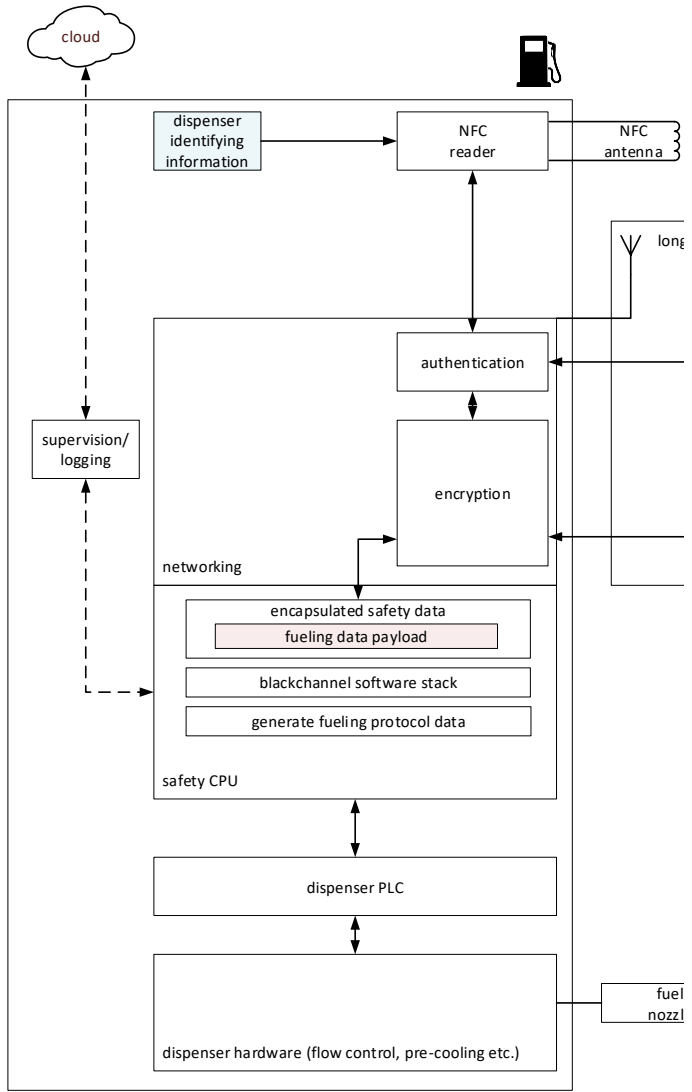
Vehicle Side Implementation

- multiple possible configurations:
  - CHSS ECU + comms ECU (new) + wireless unit (existing/new)
  - CHSS ECU (modified) + comms/wireless unit (new)
  - CHSS ECU + existing hardware on vehicle
- likely each vehicle OEM will implement differently based on EE-architecture
  - buy hardware/software and integrate
  - use existing hardware, buy software
  - use existing hardware, write own software



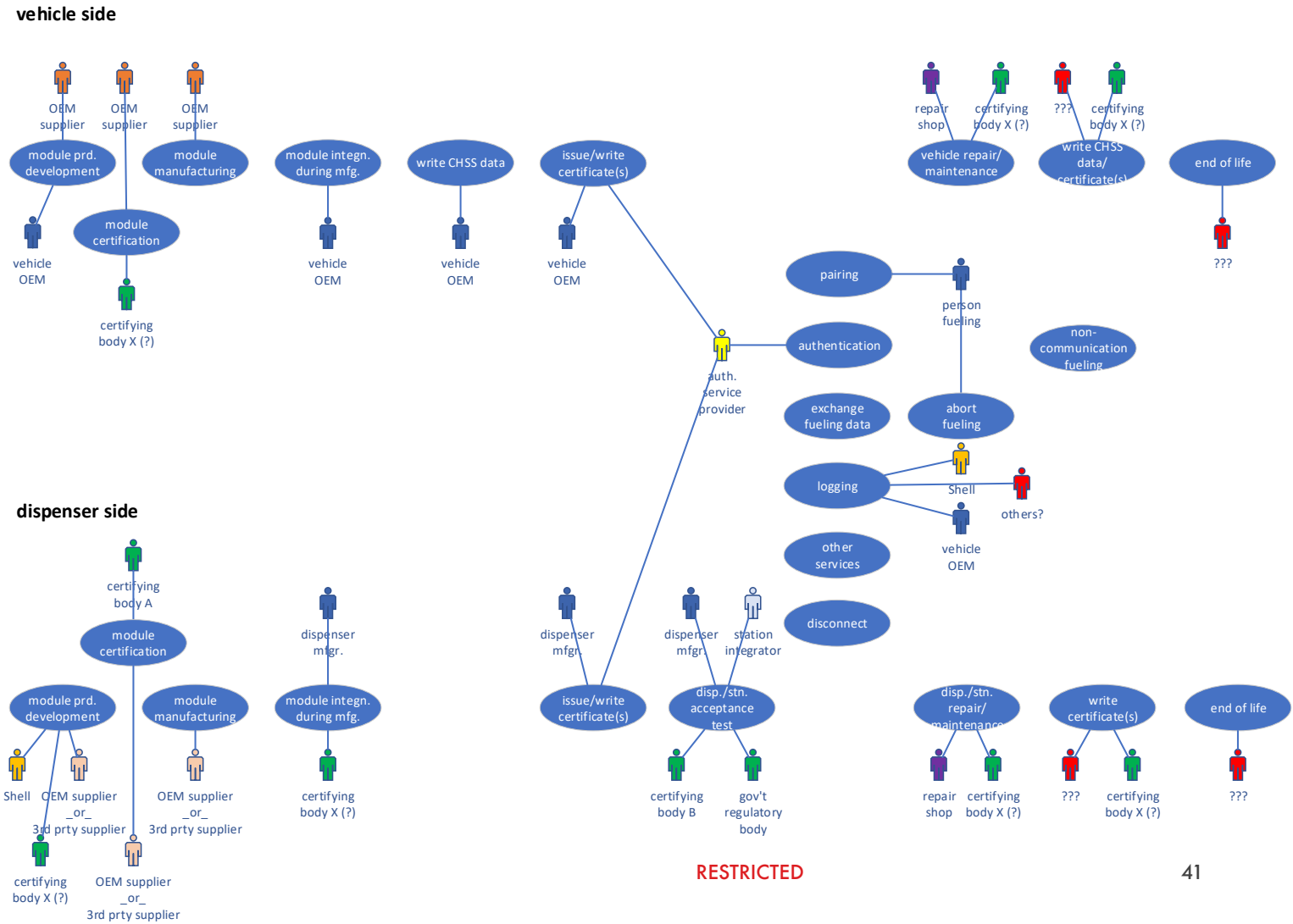
Dispenser Side Implementation

- fewer possible configurations:
  - comms unit + dispenser PLC with safe communication bus, e. g. ProfiSAFE
  - dispenser PLC and safetyCPU in once device (eliminates safe bus connection)

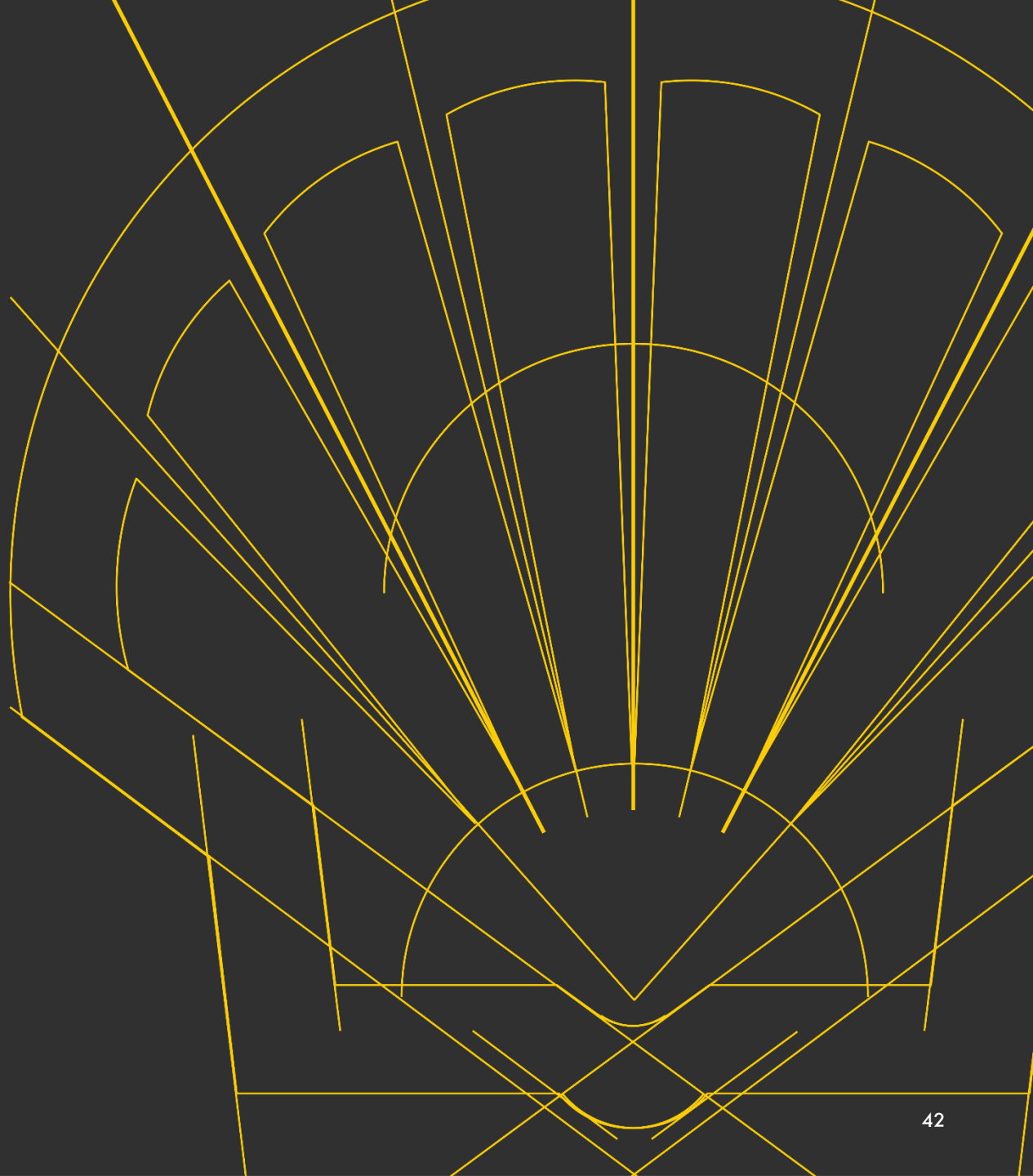


Use Case Diagram

- for the moment: taking into consideration product development activities as well
- some interactions still TBD
- main difference vehicle/dispenser: dispenser/station must pass acceptance test after construction finished



Project HyConnect



Project HyConnect – Overview

- Collaboration between Shell, Bosch and HS Aalen (university of applied science)
- Funded by Shell and Bosch
- Work packages on
  - Requirements engineering
  - Concept development incl. safety analysis
  - Pre-normative activities for communication interface
  - in the past: Proof-of-Concept based on Bosch hardware/software -> postponed until more clarity from standardization
- Make part of project results available broadly to drive industry adoption

HyConnect –Timeline

WP	Titel	Project Month 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	**Project Management**	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
1	**Dissemination & Liaison**	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
2	**Standardization**	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
2.1	Preparation	■	■	■	■	■	■	■	■																						
2.2	Technical & committee activities									■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
3	**Requirements Engineering**	■	■	■	■	■	■																								
3.1	Systems Analysis and Design	■	■	■	■	■	■																								
3.2	Pairing and Communication Req's	■	■	■	■	■	■																								
3.3	Vehicle/CHSS/dispenser Req's	■	■	■	■	■	■																								
3.4	Safety and IT security Req's	■	■	■	■	■	■																								
3.5	Req's Quantification	■	■	■	■	■	■																								
3.6	Proof-of-concept Req's	■	■	■	■	■	■																								
4	**Concept Development**			■	■	■	■	■	■																						
4.1	Wireless Technology			■	■	■	■																								
4.2	IT Security			■	■	■	■																								
4.3	Functional Safety			■	■	■	■																								
4.4	Data Protocol			■	■	■	■	■	■																						
4.5	Pairing			■	■	■	■	■	■																						
4.6	System Concept			■	■	■	■	■	■																						

Project HyConnect – "Associated Partners"

- Letter of Interest/Support from:
  - Toyota, MAN, Nikola, Daimler, BMW, Jaguar Land Rover, Air Liquide, FillnDrive, Walther Precision, NREL

- Members expected to participate in
  - Collection of current status
  - Requirements identification
  - Use case discussions

- Possibility to participate in
  - Workshops

TECHWORKS

NFC pairing - notes

- the vehicle and dispenser processors/ECUs each can have a trusted execution environment to run secure applications and communication protocols requiring encryption and secure storage of sensitive data
- the NFC tag can be a active or passive tag, can integrate a secure element, can be a secure tag
- the NFC tag can adhere to Global Platform standard(s)
- the NFC tag can be on the dispenser side or on the vehicle side/NFC reader vice versa
- the NFC reader electronics and antenna can be integrated in the nozzle or the antenna can be integrated in the nozzle and the reader electronics in the dispenser

Establishing trust - notes

- identity management: provisioning (create certificates), authentication (validate user identity), authorization (determine rights to access system), self service (updating information, passwords, repair), password/certificate management (defining passwords if needed, defining other methods of access identification), governance (define guidelines/rules), deprovisioning (revoking certificates/identities/permissions)
- public key encryption can be used, utilizing a public key infrastructure (PKI)
- rolling keys/temporary keys can potentially be used and/or stored on the NFC tag
- the NFC tag can store globally unique ID(s), certificate(s), cryptographic key(s) (public key(s)) i. e. a vehicle public key, static or rolling key(s), encrypted data, vehicle identifying information (MAC address, VIN number etc.)
- the data on the tag can be read-only or read/write

Once a connection is established – notes 1

There are a large number of possible applications/actions once a communication is established between a vehicle and a dispenser:

1. Fully automated payment can be executed
   a. The customer (pre)registers payment information
   b. Payment information is obtained by the dispenser via the secure communication link, resulting in a truly frictionless transaction (i. e. user does not have to enter any payment information)
   c. different possibilities exist:
      i. payment information can be stored in the vehicle processor and communicated to the dispenser or payment information can be stored in the cloud/on a remote server and accessed by using vehicle/customer identifying data obtained through the data link
      ii. payment services similar to Apple pay or Google pay can be imagined with the car acting as “the cell phone”
2. Different authentication methods are possible
   a. Multi-factor authentication can be used where the car itself can be used as one factor (knowledge = something only the user knows, possession = something only the user has and inherence = something only the user is)
   b. if the customer registers additional devices and agrees to them being used for transactions, these can be used as a backup for authentication (i. e. pressing OK on a cell phone/tablet/vehicle display etc.)
3. White listing is possible for automated payment or other services, i. e. the vehicle can be pre-registered to receive certain services, i. e. paying for fuel, receiving a car wash etc. at certain locations (fueling stations/dispensers etc.); receiving these services might not need internet connectivity (whereas otherwise it might)
4. A large range of fleet solutions is possible
   a. Data logging (fuel consumption, payment, fuel delivery, cost splitting, fueling data, fueling operational data, vehicle/tank properties etc.) can be performed for future analysis/optimization/safety improvement etc. (not only for fleets but also to improve the station operations)
   b. Status information can be submitted for repair/maintenance, i. e. for oil/fluids change etc.
   c. if the communications interface has access to other vehicle data these can be accessed and processed
   d. real time data can be sent to fleet operator
   e. electronic driving logs can be managed/transmitted etc.

Once a connection is established – notes 2

1. A data storage can be added to the vehicle that can be used to store any data; a data wallet can be placed on board of the vehicle
   a. private data/fleet data
   b. fueling data
   c. government data such as TUV certificates, inspection data
   d. store maintenance records
   e. data can be stored for commissioning of vehicles
2. Additional services can be offered
   a. convenience, i. e. pre-prepare coffee, reserve a shower for driver etc.
   b. for ride sharing: rider refuels and gets bonus points, general management etc.
   c. offers can be sent to other mobile devices/email addresses etc.
3. On demand transport services can be implemented, i. e. taking packages from service station A to service station B if the route is known
4. Displays can be used to show additional information, i. e. using the display inside a vehicle, on the dispenser, on the nozzle, on a cell phone/tablet/other mobile device
   a. local info
   b. info from fleet base
   c. personalized into based on vehicle information
   d. display fueling time/duration to driver
   e. display ads/offers
5. Customer loyalty programs can be applied automatically, i. e. bonus points/money, digital fleet cards, special conditions, etc.
6. An alert can be given on any additional mobile device such as a cell phone when the fueling is done