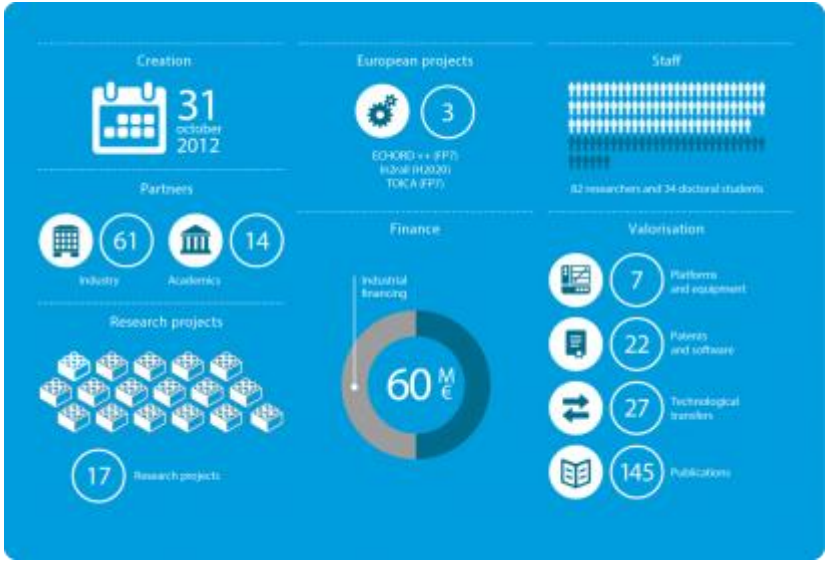
Towards a Common Architecture Framework for ITS

Antonio Kung – Trialog

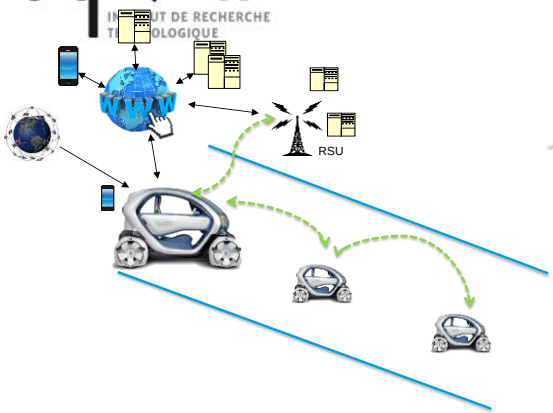
With the participation of

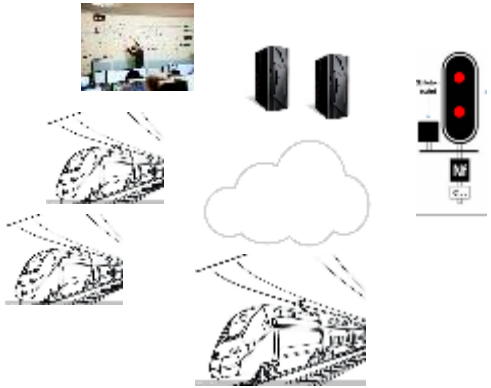
Witold Klaudel – Project leader (Renault), Antoine Boulanger (PSA), Cyril Grépet (Trialog), Christophe Jouvray (Valeo), Laura Rodriguez (Airbus), Benjamin Venelle (Valeo).

- **SystemX – French Institute for technology research**
  - Creation: 2012
  - Focus: Digital engineering of complex system
  - Approach: Industry collaboration
- **CTI – Cybersecurity of Intelligent Transport**
  - One project of SystemX
  - June 2016 – 4 years.
- **Trialog**
  - SME focusing on engineering of complex system, member of CTI



Three Domains: Automotive, Aeronautics, Railway





New functions
- Driving: assistance, automation, cooperative decisions
- Concierge service, diagnosis, remote update / repair, e-call
- Internet connectivity and on-board services

Privacy protection
- Privacy regulation compliance
- Privacy-by-design and citizen empowerment

New security threats
- Drastic increase in attack surfaces
- **Direct impact on safety**
- Complexity of preparation of the attacks but simplicity of their execution, knowledge accessibility
- Cybercrime in organized crime and terrorism

New responsibilities and regulatory constraints

Cybersecurity of Intelligent Transports (CTI)

Application domains: aeronautic, automotive, railways


AIRBUS


PSA GROUPE
RENAULT
Valeo


RATP
ALSTOM

- **Objective: Addressing the security of intelligent transports**
  - Three industries with “similar” architecture and safety concerns
  - Promote a “common” architecture and practices for the 3 domains

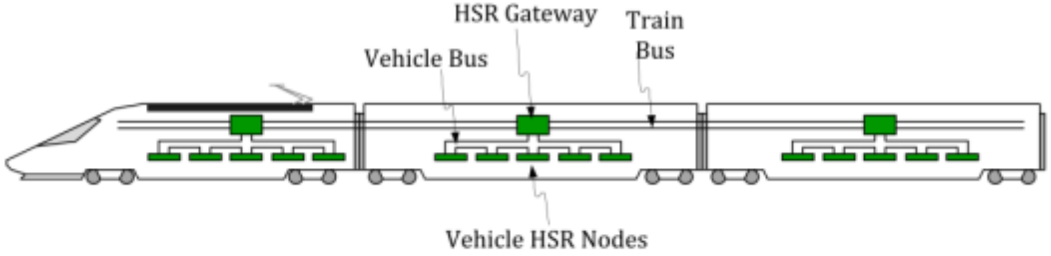
Digital Security
Une société du Groupe Econocom
IDNOMIC
TRIALOG
PROVE & RUN

Small and medium-sized enterprises

Gendarmerie nationale

National agencies

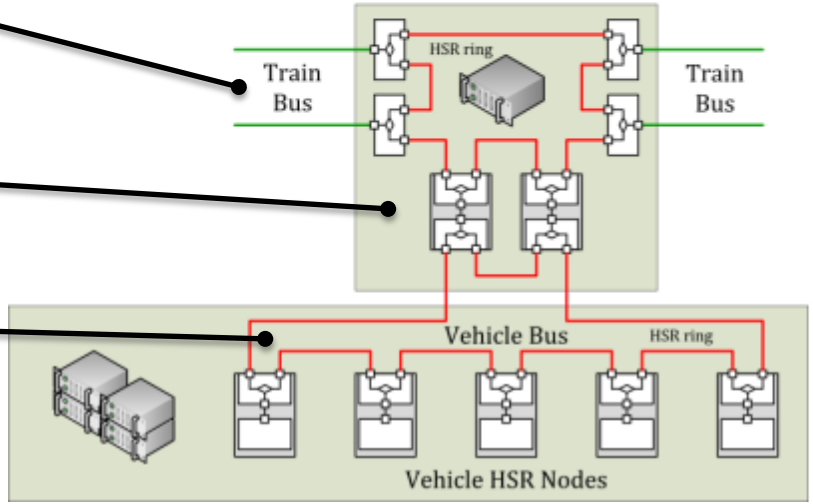
Current transport architectures

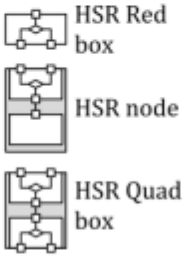


High-speed backbone

Network gateways

Dedicated networks





All devices are based on HSR/PRP

Switch IP

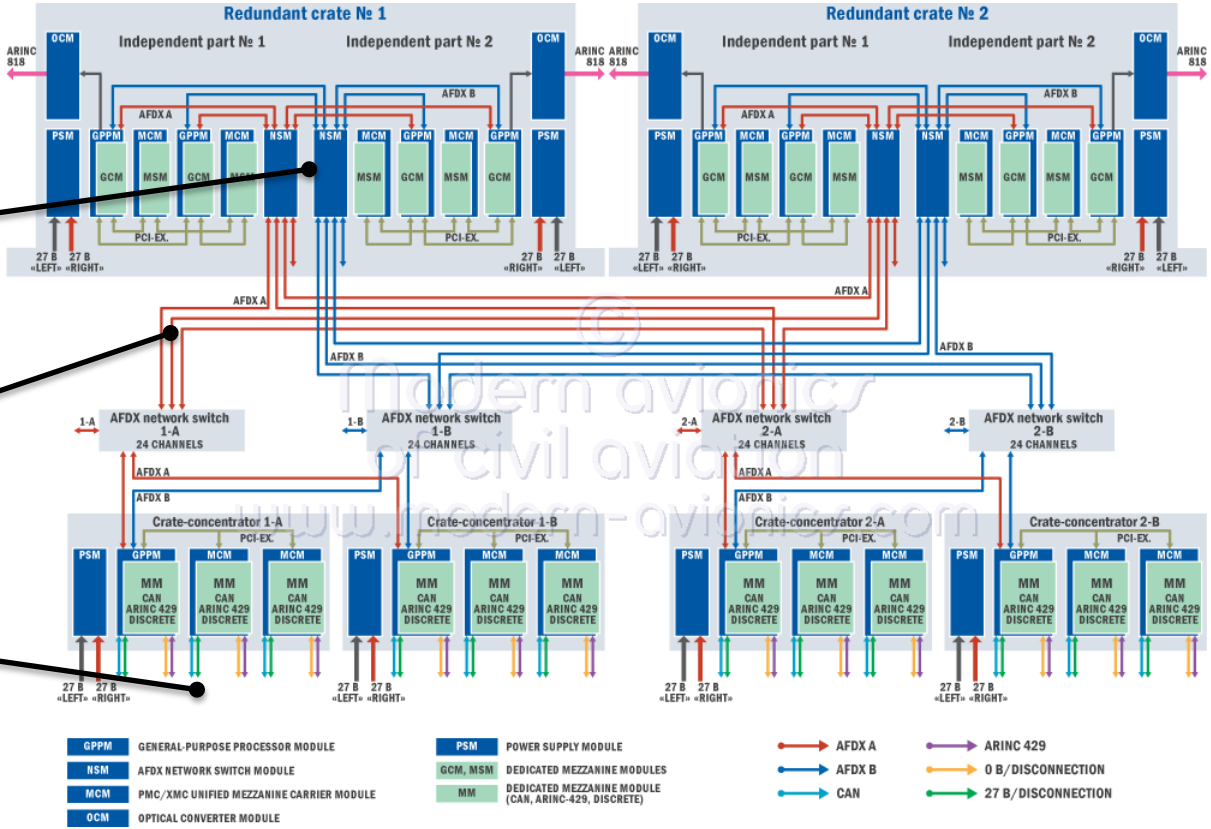
Courtesy soc-e.com

Current transport architecture

Network gateways

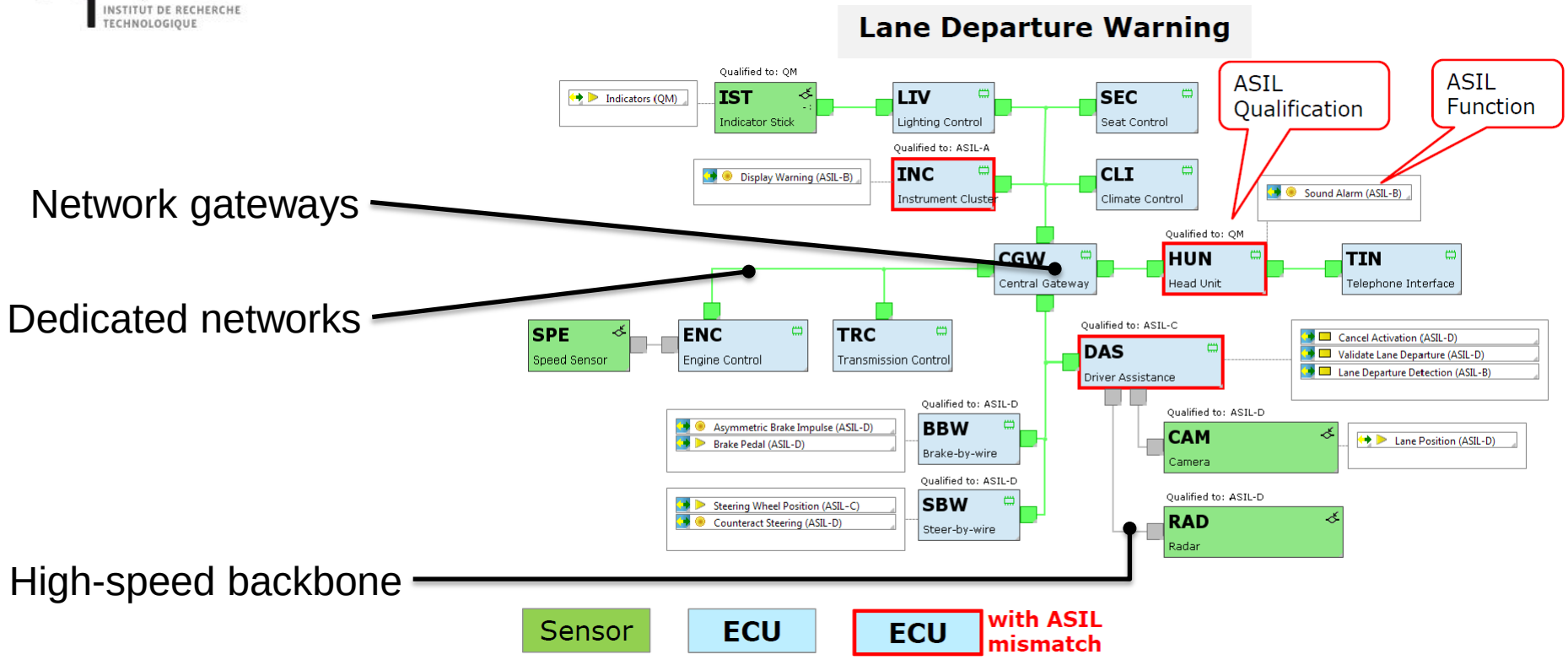
High-speed backbone

Dedicated networks



Courtesy modern-avionics.com

Current transport architecture



Courtesy vector.com

Current transport architecture

Distinct businesses but similar system elements



Controllers	Avionic & Flight systems Mission & Payload	Core Vehicle Services Infotainment	CBTC signaling, … Passenger information, …
Radios	UAV to command center UAV fleet cooperation	Vehicle to Infrastructure (V2I) Vehicle to Vehicle (V2V)	Train to Supervision/Maintenance Train to Infrastructure Signaling
Sensors	Altimeter, Airspeed, Sonar, … GPS, VOR/ILS, DME, …	Camera, LIDAR, … Galileo, GPS, …	Signaling balises, … Odometer, beacons, …
Networks	ARINC 429 & MIL-STD-1553 ↓ Ethernet (AFDX)	CAN, LIN, Flexray ↓ Ethernet (BroadR-Reach)	Ethernet (PRP & HSR)

Similar attacks for all domains

Lessons learned

Security need analysis

Main perception means

https://en.wikipedia.org/wiki/Iran–U.S._RQ-170_incident

- **2011 – CIA's drone hijacked by Iran**
  - Lockheed Martin RQ-170 Sentinel
  - GPS spoofing to force drone to land

- **2012 – Fatal UAV crash in South Korea**
  - Schiebel S-100 Camcopter
  - GPS jamming (from North Korea ?)

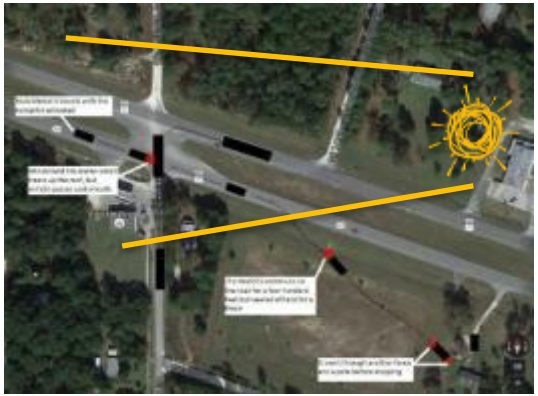
https://www.suasnews.com/2012/05/schiebel-s-100-crash-kills-engineer-in-south-korea/

Sensors can be fooled or jammed
Enforce sensor fusion against fault injection

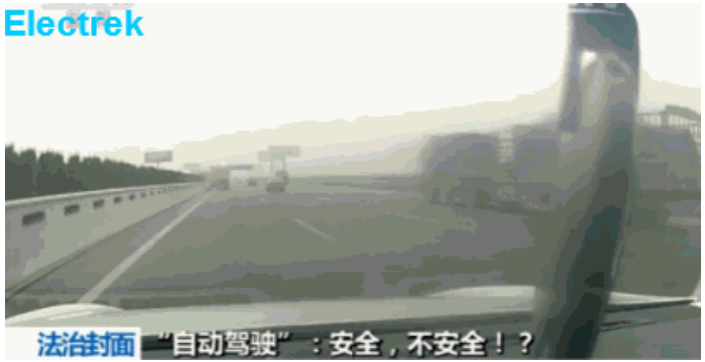
Security need analysis

Main perception means

- **2015 – LiDAR can be fooled by fake echoes**
- **2016 – Fatal Tesla accidents in China and Florida**
  - Obstacle misdetection (China)
  - Blind camera (Florida)



https://electrek.co/2016/07/01/understanding-fatal-tesla-accident-autopilot-nhtsa-probe/



https://electrek.co/2016/09/14/another-fatal-tesla-autopilot-crash-emerges-model-s-hits-a-streetsweeper-truck-caught-on-dashcam/

Authenticate onboard devices to vehicle

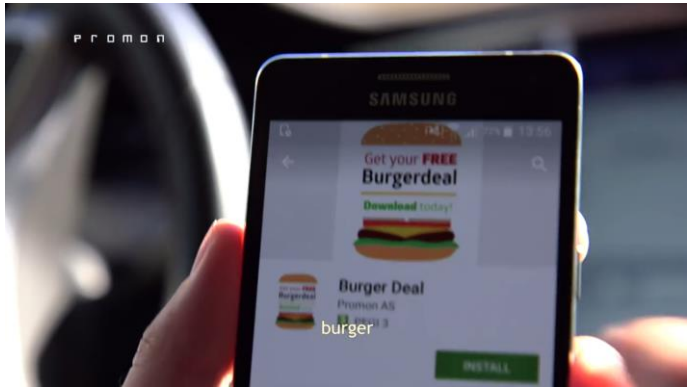
Security need analysis

Main communication channels

http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

- **2016 – Remote attack on Tesla**
  - 0-day in the communication unit
  - Direct access to vehicle internals

- **2016 – Tesla's remote control**
  - Rogue wifi hotspot at restaurant
  - Free burger if you install this app
  - Malicious app drives Tesla's app



https://promon.co/blog/tesla-cars-can-be-stolen-by-hacking-the-app/

Isolate vehicle internals from exposed devices
Enforce network control & authentication

Security need analysis

Main embedded services

http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

- **2015 – Remote attack on Jeep**
  - Anonymous access to infotainment
  - Malicious update of a critical controller
- **2016 – 1.4M of car were recalled by GM**
  - 0-day in IVI systems of Chrysler, Dodge, Jeep and Ram
  - Estimated time: 5 years
  - Connected cars by 2022: 203M

http://www.allpar.com/corporate/tech/firmware-updates.html

Speeding up security fix delivery to reduce exposure
Isolation btw privileged and less privileged ECUs

Achieved Work

Common use cases

Taxonomy of topics

Principles on on architecture

- **Use case viewpoints**
  - Main IOT perception means
  - Main communication channels
  - Main embedded devices
  - On-board storage and shared services
- **Identification of threats for each viewpoints**
- **Identification of principles for mitigation**

[2] Common description of use cases and threats

Main perception means

Robustness of the system against sensors

- **Camera, LIDAR, …**
- **Galileo, GPS, …**

- **Altimeter, airspeed, sonar, …**
- **GPS, VOR/ILS, DME, …**

- **Balise reader**
- **Odometer**

Environment analysis

Protect system from rogue sensors

Positionning system

Main communication channels

Robustness of the system against Byzantines

- Vehicle to infrastructure (V2I)
- Vehicle to vehicle (V2V)

- UAV to command center
- UAV fleet cooperation

- Train to Supervision or Maintenance
- Train to Infrastructure Signalling Controllers

Mid to long range

Isolate networks by their purpose

Short to mid range

Non-safety related

Safety related

Main embedded services

Robustness of the system against malicious freight/passenger

- **Core vehicle services**
- **Infotainment**

- **Avionic/Flight controller**
- **Mission/Payload controllers**

- **CBTC Signalling**
- **Passenger Information, Voice, CCTV…**

Core sub-systems

Isolate systems by their privilege level

Freight/passengers/information sub-systems

Onboard data storage & Shared services

Mitigates with system failures & 0-days

- **Event data recorder (EDR) & system logs**
- **Update over the air (OTA)**

- **Flight data recorder (FDR)**
- **UAV recall for updates (??)**

- **Event data recorder (EDR)**
- **System logs remote download**
- **Update over the air (OTA)**

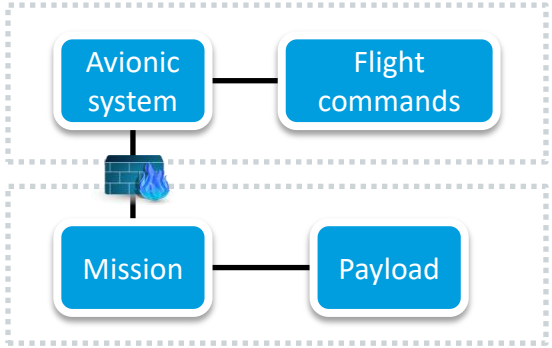
Forensic & diagnosis

Update management policy

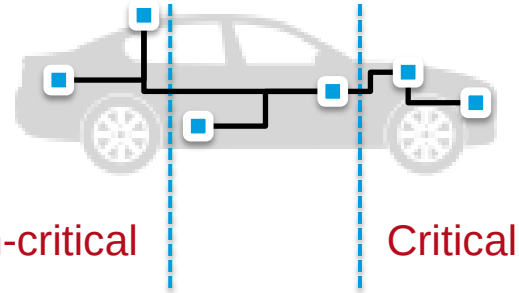
Various isolation strategies

Main embedded services

- **Certified/non-certified isolation**
  - No access to certified controllers
  - Legal constraint for aeronautic systems

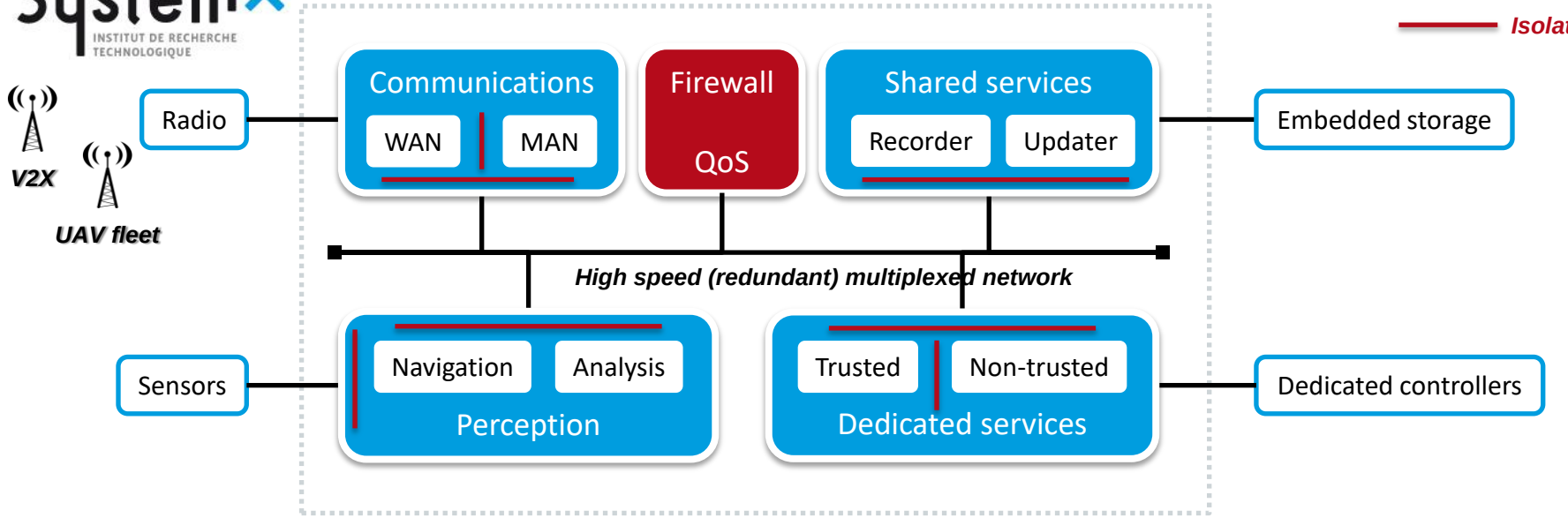


- **Safety/non-safety isolation**
  - Controller segregation by their safety level
  - Legal constraint for railway systems



- **Critical/non-critical isolation**
  - ECU distribution by their criticality level (natural)

Common Functional Organization



- **Internal work**
  - Architecture
  - Demonstration
- **Community work**
  - Contribution 1 (now):
    - Towards common use case template
    - Towards common architecture framework
  - Contribution 2 (in the future):
    - Towards common cybersecurity process

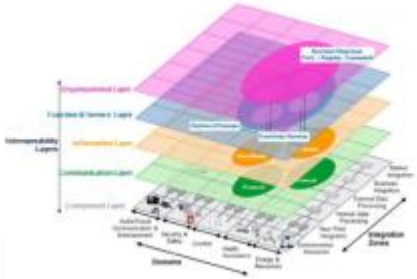
Community Work

Towards common use case template

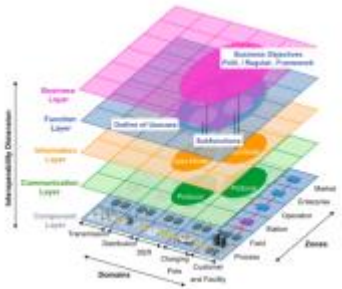
Towards common architecture framework

Principle: Use Architecture Models

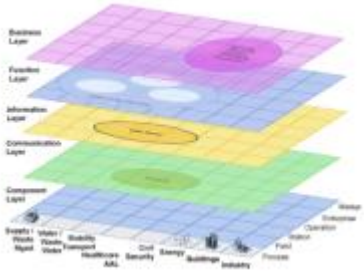
- **Home and building architecture model (HBAM)**
  - http://www.corenetix.com/downloads/german-standardization-roadmap-smart-home---building--version-2-0-data.pdf



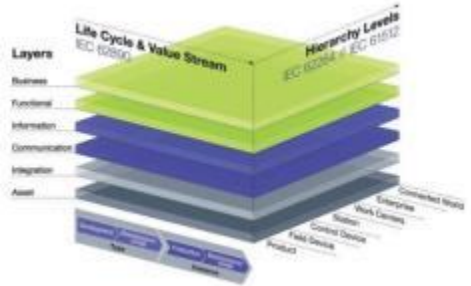
- **Electric mobility architecture model (EMAM)**



- **Smart City Infrastructure architecture model (SCIAM)**
  - https://www.dke.de/resource/blob/778248/d2afdaf62551586a54b3270ef78d2632/the-german-standardization-roadmap-smart-city-version-1-0-data.pdf

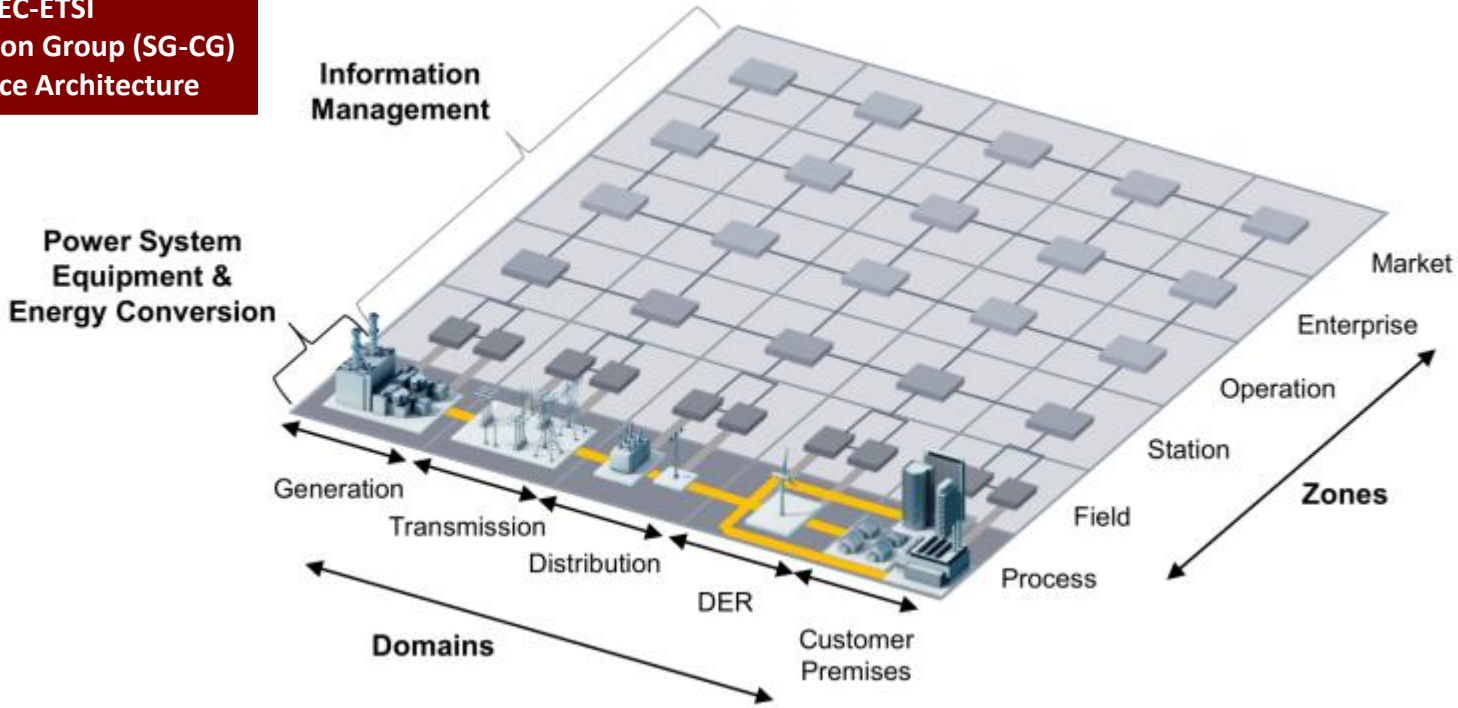


- **Reference Architecture Model Industry 4.0 (RAMI)**
  - https://www.zvei.org/en/subjects/industry-4-0/the-reference-architectural-model-rami-40-and-the-industrie-40-component/



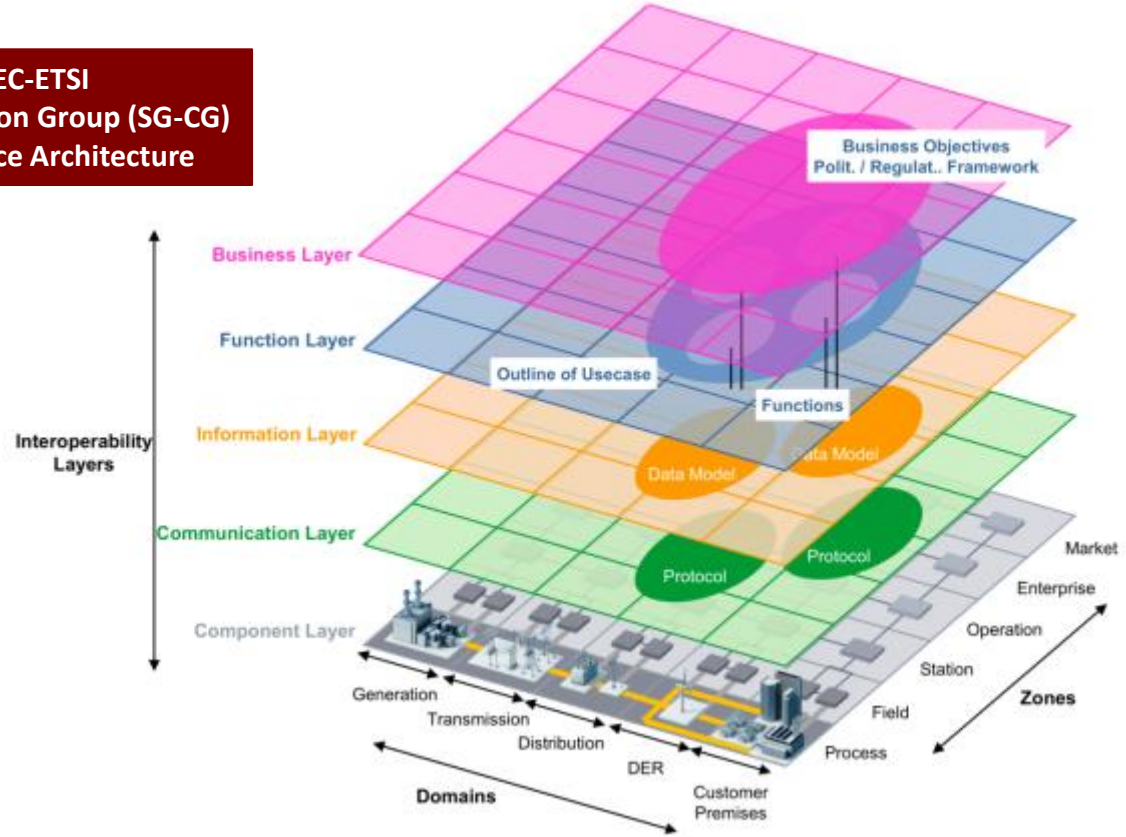
Example of Smart Grid Architecture Model

CEN-CENELEC-ETSI
Smart Grid Coordination Group (SG-CG)
Smart Grid Reference Architecture

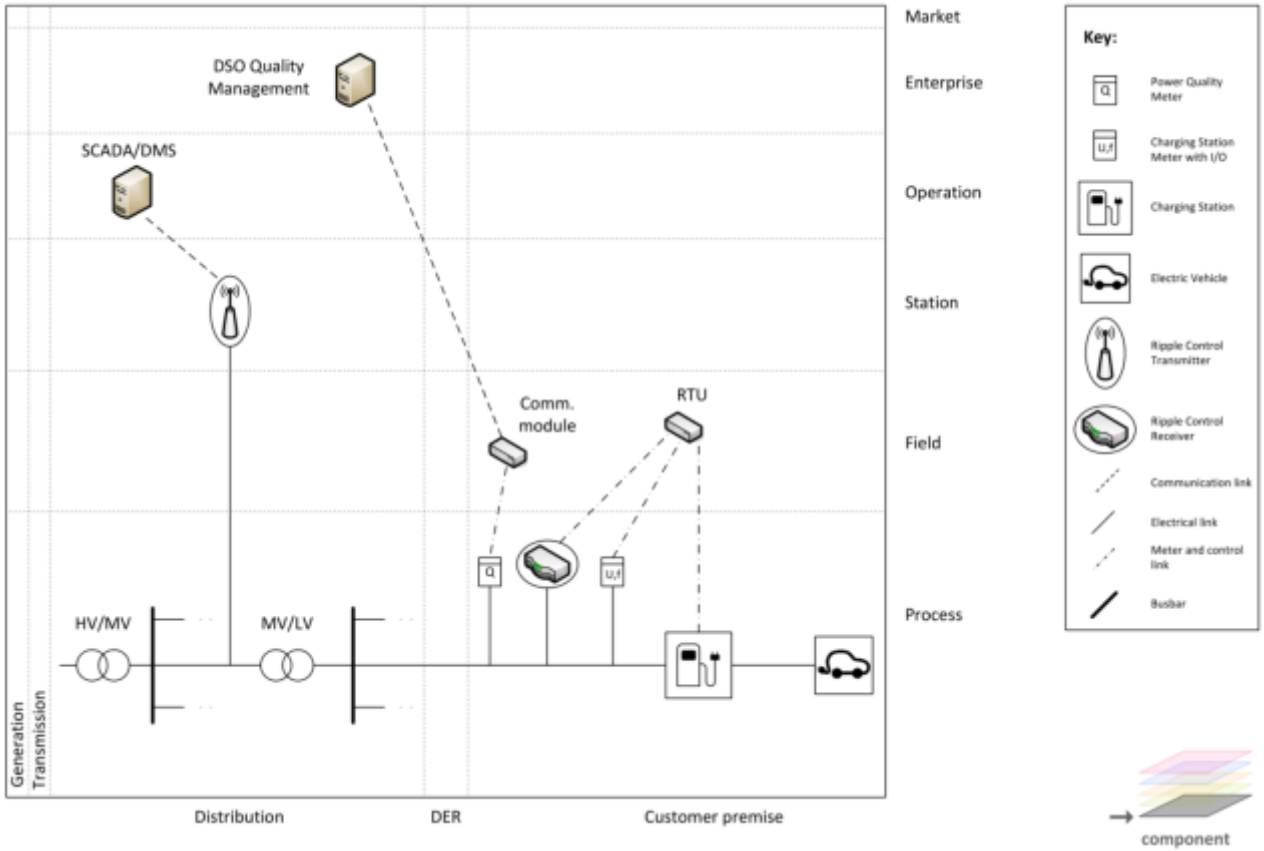


Smart Grid Architecture Model (SGAM)

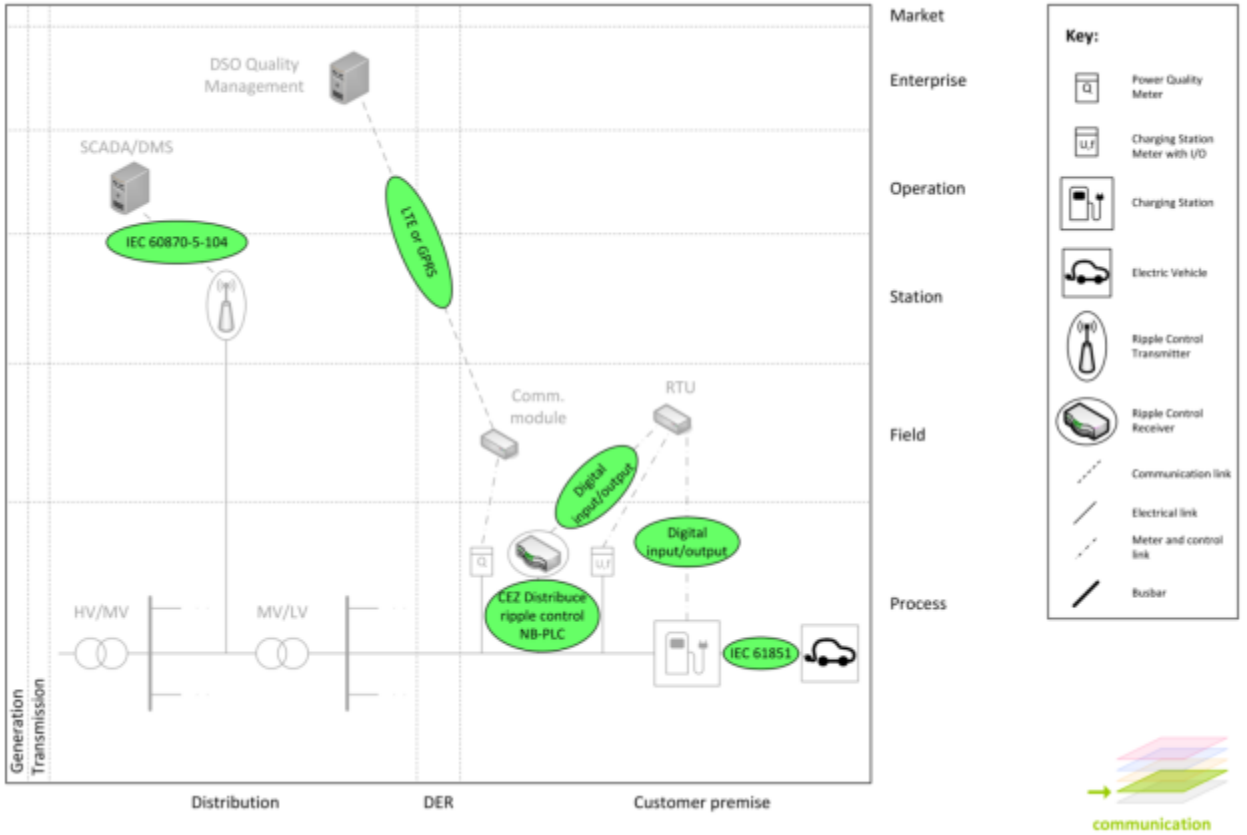
CEN-CENELEC-ETSI
Smart Grid Coordination Group (SG-CG)
Smart Grid Reference Architecture



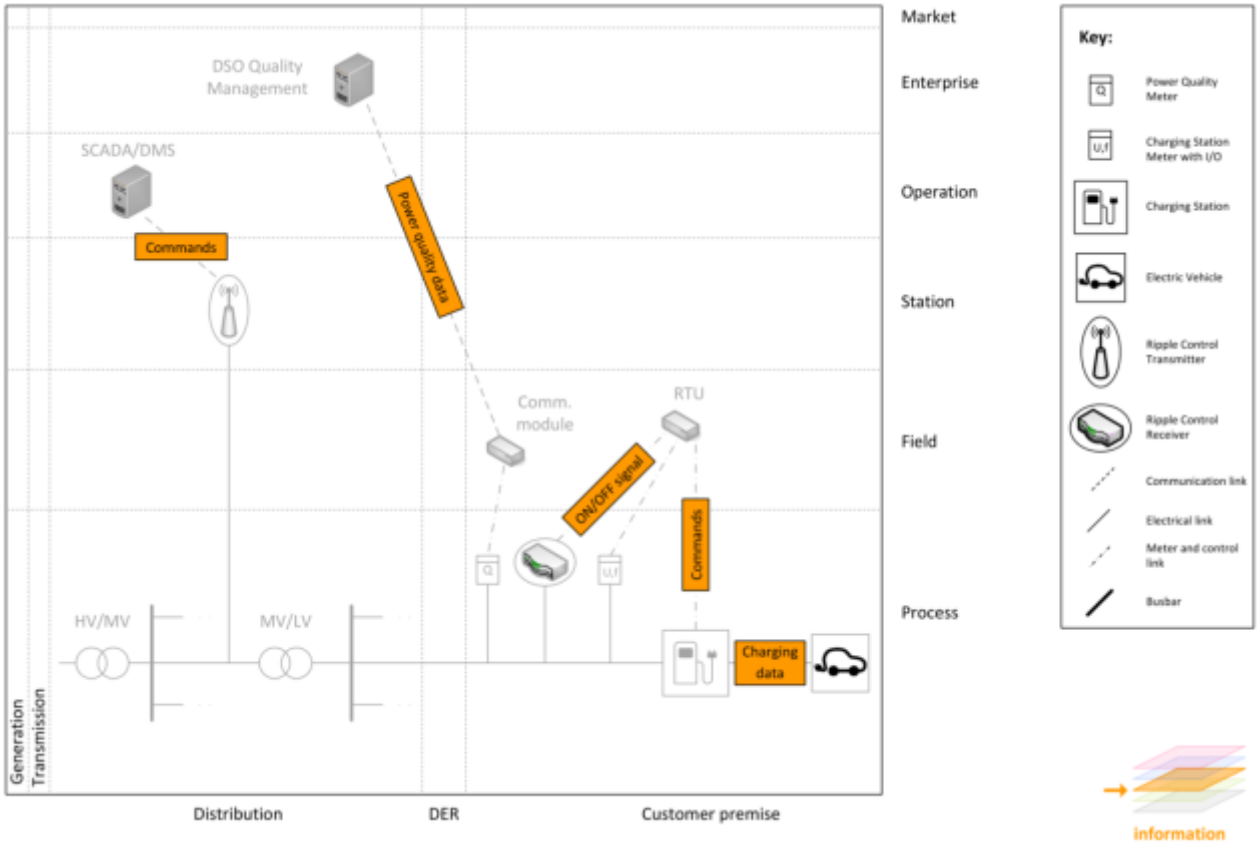
Example of EV charging component plane



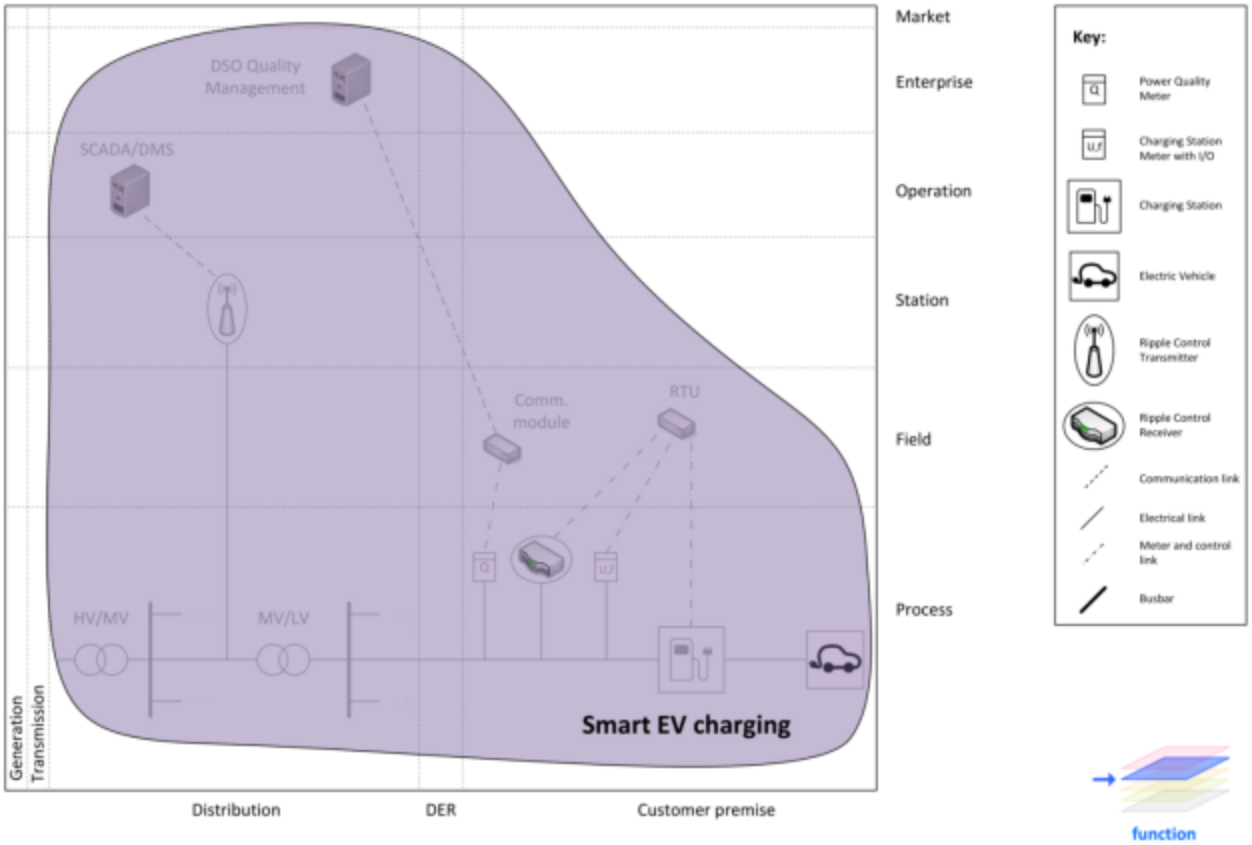
Example of EV charging (Communication Plane)



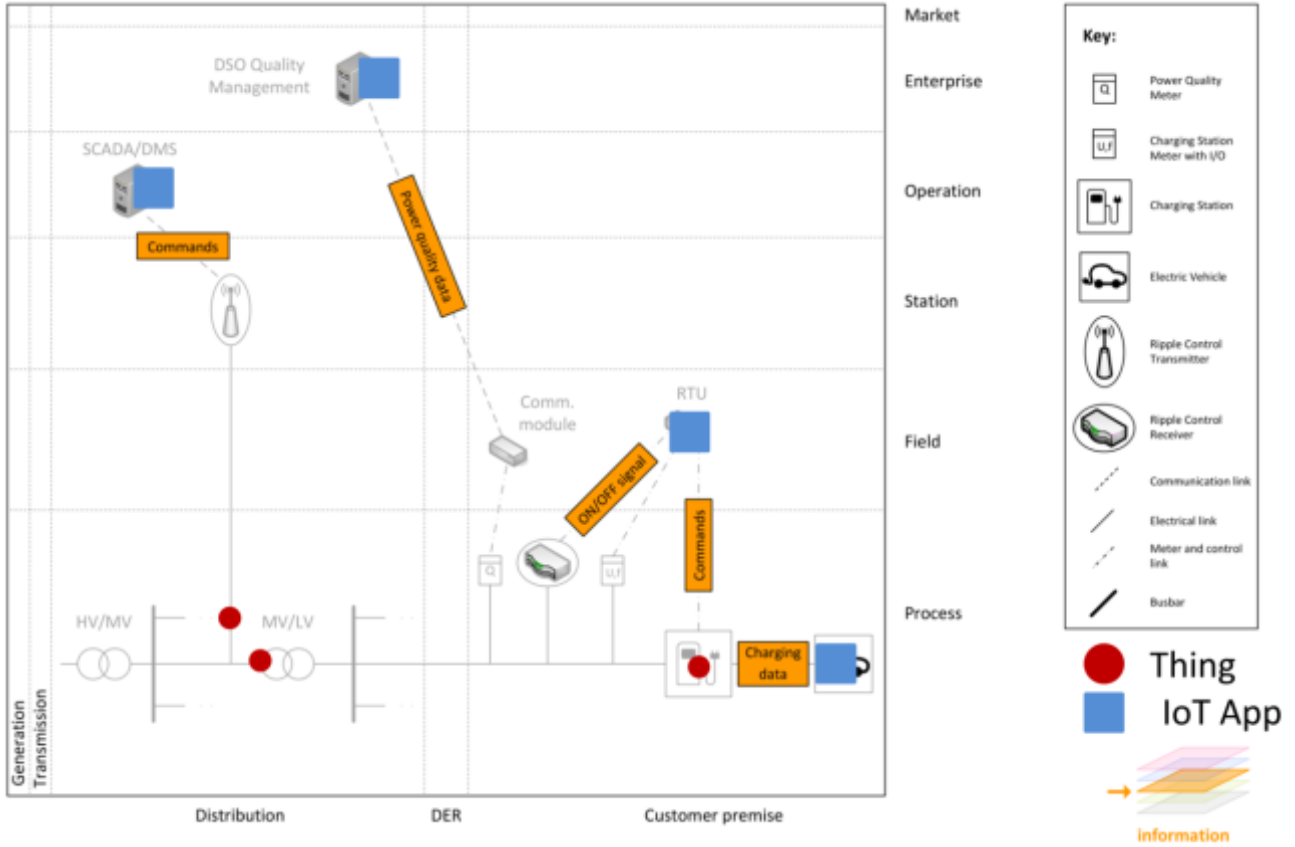
Example of EV charging (Information Plane)



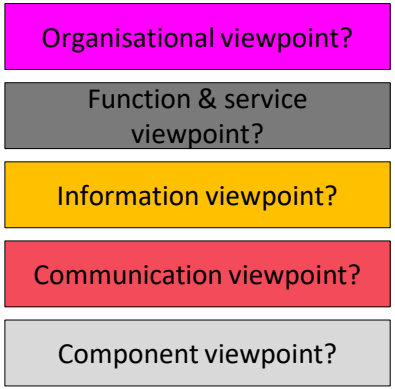
Example of EV charging (Function)

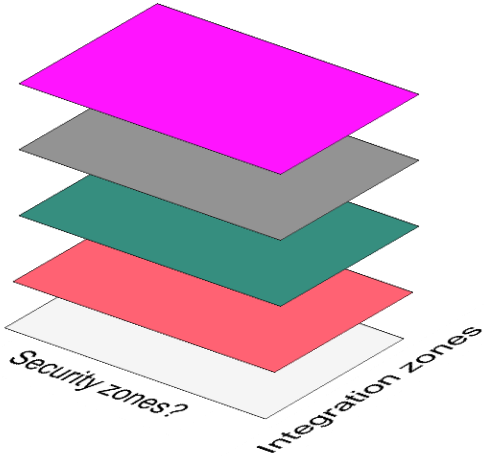


IoT in the Smart EV charging Information plane

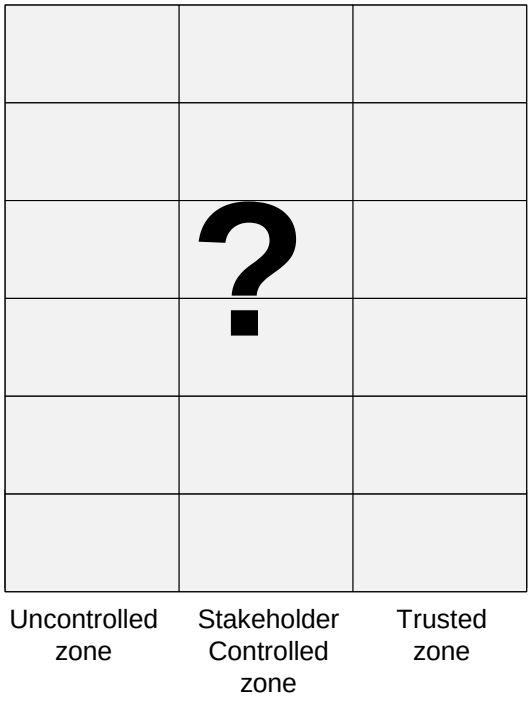


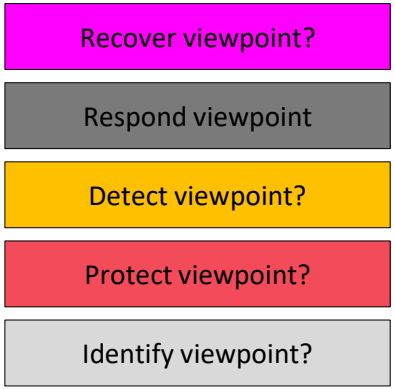
- Three dimension approach
- Integration of misuse cases
- Integration of life cycle
  - Identify, protect, detect, response, recover
- Integration of security and safety

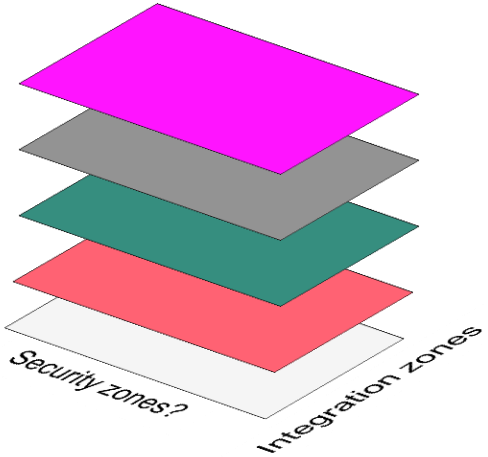




Examples


?
Market integration
Business integration
External Data processing
Internal Data processing
Near-field interaction
Environmental interaction
Uncontrolled zone
Stakeholder Controlled zone
Trusted zone


Recover viewpoint?
Respond viewpoint
Detect viewpoint?
Protect viewpoint?
Identify viewpoint?


Security zones?
Integration zones

Work to be done

- Investigate several templates
- Describes the same use case for each template
- Align with a common cybersecurity architecture model

Thanks

Antonio Kung. www.trialog.com

http://www.irt-systemx.fr/en/