Security Conference 2022

Traffic Data and Vehicles as IoT Sources

Massimiliano Masi – Autostrade Per L'Italia SpA

04/10/2022

THE ROLE OF A MOTORWAY OPERATOR

THE CONTEXT

Road Operators are considered **critical infrastructures** in some countries.

- Service Disruptions **impact other critical infrastructure** [*ENISA*]
- **Service is delivered through IT/OT/IoT** infrastructure: Variable Message Signs, C-ITS, Red lights. Such data is used for *Traffic Management Plans*
- **Road operators are interconnected** indirectly through National Access Points and directly to exchange Real Time Traffic Information (RTTI) and Safety Related Traffic Information (SRTI)
- It is also a **typical company**, with IT systems: endpoints, ERP, social networking

PECULIARITIES

- **Usually operates Optic Fiber-based network** equipment, geographically distributed
- Energy supply, Diesel Engines, Radio Equipment, Charging Stations

IMPACTS

- **Network congestion** could cause pressure on other adjacent infrastructures (Hospitals, Smart Cities, Good delivery), and causes **vehicle crashes**
- **Malfunctioning** on a Road Tunnel IoT/OT equipment can cause **injuries** and **deaths**

[ENISA] Good Practices on Interdependencies between OES and DSPs, Nov. 2018

DATA SOURCES

Road Operators manages traffic data

- License Plates (either individual or commercial), geolocation data, traffic data flows (enforceable by law – speed limit checker)
- Speed, direction of identifiable vehicles
- Dynamical weight of vehicles
- CCTV
- Environmental sensors on bridges, tunnels

A special case: C-ITS

- Cooperative Intelligent Transport System: Vehicle and Infrastructure exchange data either through 5G or via Direct Short-Range Communications
- Vehicles' C-ITS stations (On Board Units) share **Cooperative Awareness Messages** (CAM) with other vehicles and Infrastructure's Fixed C-ITS Stations (RoadSide Units)
- CAM message may contain speed, direction, and events of the Vehicle.
- Messages are signed by a certificate issued by an external IEEE 1609.2 PKI and changed "often". The CN is a pseudonym
- **The pseudonym can't identify a vehicle** from a Road Operator's knowledge**, but it becomes PII** if Vehicle Manufacturer and Road Operators agree on profiling

Road Operators are not regulated: no Norm exists (e.g., like the CEN CLC 50701)

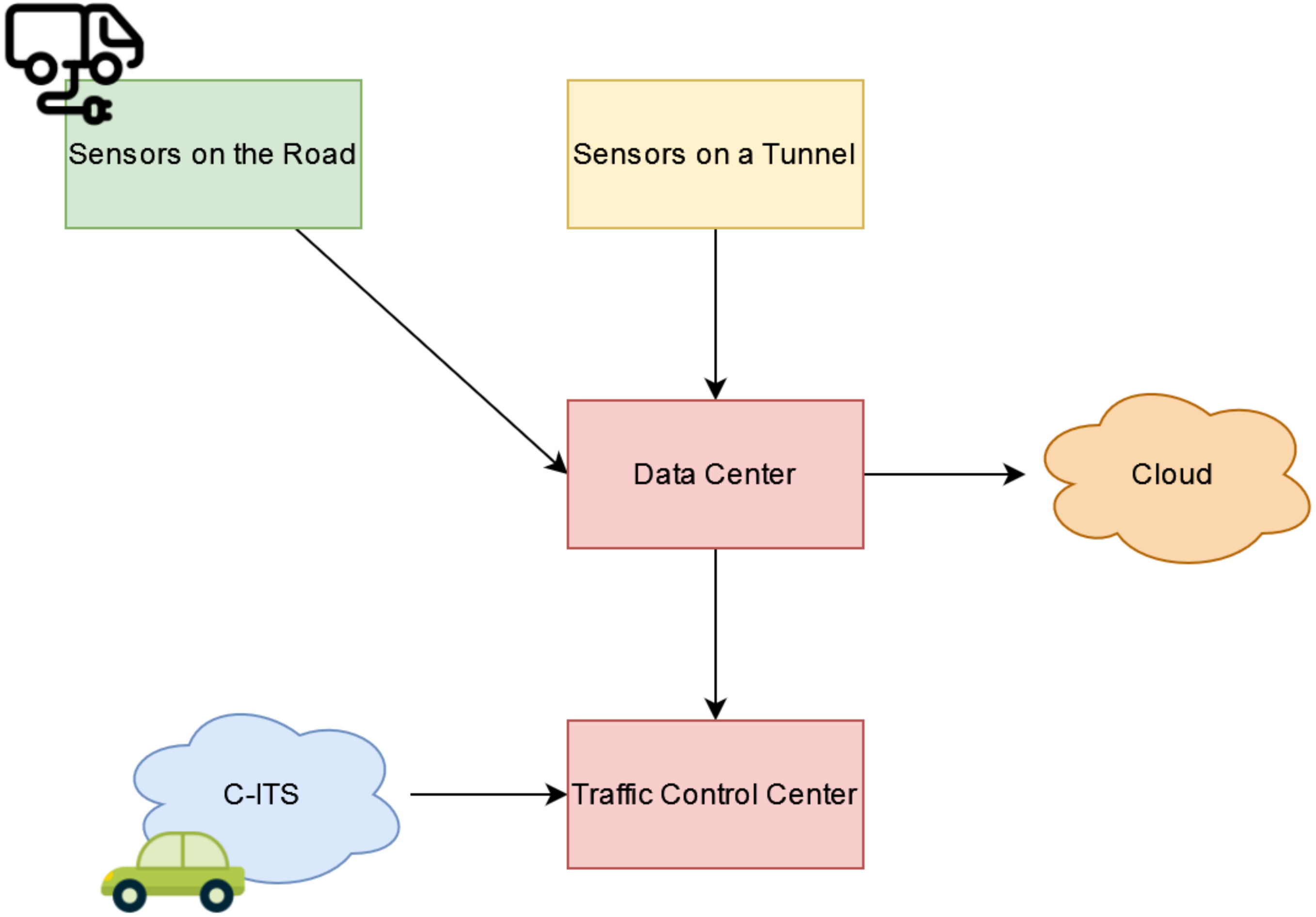
DATA FROM DIFFERENT SECURITY DOMAINS

Typical data journey

- **Read from a sensor on the road** (IoT). Data is semantically and syntactically different (e.g., CCTV, LoraWAN).
- **Sensors and actuators in Tunnels**. Data is exchanged using OT protocols from IoT devices, actuating tunnel pumps in case of fire.
- Data arrives in a Data Center or in a Cloud VPC. **Risks related to cloud** have to be considered
- Data is elaborated in a Traffic Control Center:Traffic Management Plans, SRTI, RTTI, send Hazardous Location Notification
- C-ITS data arrives at 10hz per vehicle **over a public network** (DSRC)

According with IEC 62443, those may have different Security Level Target (SL-T)

- This means different countermeasures on integrity, confidentiality
- How to trust data from C-ITS? Security Policy only requires a "ISO 27001 certification"



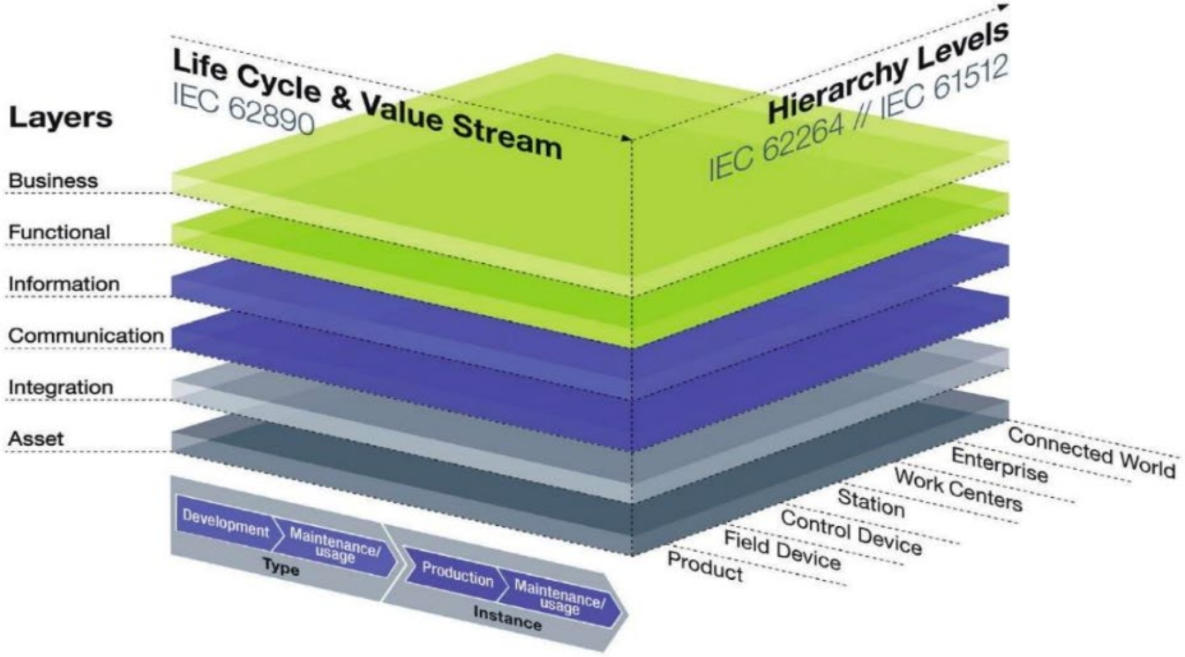
RAMI, 27001, 62443

Use of IEC 62443

- Mapping all the abstract architectural assets to the RAMI 4.0 framework
- Use Business and Functional as target for the **high-level risk analysis**
- Use Communication as hint for **zone and conduit**
- Use integration and assets to select the items for the **low-level risk analysis**
- Perform security testing

The 27001 protection rings

- Multi-compliance: security zones share 27001 and 62443 requirements
- Use of the NIST Cybersecurity Framework as a mapping tool
- IEC 62443-2-1 and the related TR, should be updated



TAKE HOME

- Data used for Traffic Management has different sources with different security level targets
- No Cybersecurity standard, or norm, exists as guidance among the Road Operators
- C-ITS, with data shared from vehicles, will dramatically improve the accuracy of Traffic Information