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

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

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

New responsibilities and regulatory constraints

August 28, 2017
Towards a Common Architecture Framework for ITS
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

Small and medium-sized enterprises  
National agencies
Current transport architectures

- High-speed backbone
- Network gateways
- Dedicated networks

Courtesy soc-e.com
Current transport architecture

Network gateways

High-speed backbone

Dedicated networks

August 28 2017
Towards a Common Architecture Framework for ITS
Current transport architecture

Network gateways

Dedicated networks

High-speed backbone

Lane Departure Warning

ASIL Qualification

ASIL Function

August 28 2017
Towards a Common Architecture Framework for ITS
Slide 7
## Current transport architecture

### Distinct businesses but similar system elements

<table>
<thead>
<tr>
<th>Controllers</th>
<th>Avionic &amp; Flight systems</th>
<th>Core Vehicle Services</th>
<th>CBTC signaling, ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission &amp; Payload</td>
<td>Infotainment</td>
<td></td>
<td>Passenger information, ...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Radios</th>
<th>UAV to command center</th>
<th>Vehicle to Infrastructure (V2I)</th>
<th>Train to Supervision/Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAV fleet cooperation</td>
<td>Vehicle to Vehicle (V2V)</td>
<td>Train to Infrastructure Signaling</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sensors</th>
<th>Altimeter, Airspeed, Sonar, ...</th>
<th>Camera, LIDAR, ...</th>
<th>Signaling balises, ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS, VOR/ILS, DME, ...</td>
<td>Galileo, GPS, ...</td>
<td>Odometer, beacons, ...</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networks</th>
<th>ARINC 429 &amp; MIL-STD-1553</th>
<th>CAN, LIN, Flexray</th>
<th>Ethernet (PRP &amp; HSR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet (AFDX)</td>
<td>Ethernet (BroadR-Reach)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Similar attacks for all domains

Lessons learned
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?)

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

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

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

Authenticate onboard devices to vehicle
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

Isolate vehicle internals from exposed devices
Enforce network control & authentication
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

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 architecture
Approach

- **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

- Camera, LIDAR, ...
- Galileo, GPS, ...
- Altimeter, airspeed, sonar, ...
- GPS, VOR/ILS, DME, ...
- Balise reader
- Odometer

Robustness of the system against sensors

- Environment analysis
- Protect system from rogue sensors
- Positioning system

August 28 2017
Towards a Common Architecture Framework for ITS
Main communication channels

- 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

Robustness of the system against Byzantines

- Mid to long range
- Short to mid range
- Isolate networks by their purpose
- Non-safety related
- Safety related
Main embedded services

- Core vehicle services
- Infotainment
- Avionic/Flight controller
- Mission/Payload controllers
- CBTC Signalling
- Passenger Information, Voice, CCTV...

Robustness of the system against malicious freight/passenger

Core sub-systems

Isolate systems by their privilege level

Freight/passengers/information sub-systems
Onboard data storage & Shared services

- 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)

Mitigates with system failures & 0-days

Forensic & diagnosis

Update management policy
Various isolation strategies

- **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

- **Communications**
  - WAN
  - MAN

- **Firewall**
  - QoS

- **Shared services**
  - Recorder
  - Updater

- **Embedded storage**

- **High speed (redundant) multiplexed network**

- **Sensors**
  - Navigation
  - Analysis

- **Perception**

- **Dedicated controllers**
  - Trusted
  - Non-trusted

- **Dedicated services**

- **Radio**

- **UAV fleet**

- **V2X**

- **Isolation**

August 28 2017  Towards a Common Architecture Framework for ITS  Slide 24
Future Work

- 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)**

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

- **Smart City Infrastructure architecture model (SCIAM)**

- **Reference Architecture Model Industry 4.0 (RAMI)**
Example of Smart Grid Architecture Model

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

August 28 2017 Towards a Common Architecture Framework for ITS
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
To Study

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

Organisational viewpoint?
Function & service viewpoint?
Information viewpoint?
Communication viewpoint?
Component viewpoint?
### Example: SystemX - Towards a Common Architecture Framework for ITS

#### Uncontrolled zone
- Stakeholder
- Controlled zone
- Trusted zone

<table>
<thead>
<tr>
<th>Environment</th>
<th>Market integration</th>
<th>Business integration</th>
<th>External Data processing</th>
<th>Internal Data processing</th>
<th>Near-field interaction</th>
<th>Environmental interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled zone</td>
<td>Integration zones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*August 28, 2017*
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/