V2X

Infrastructure for Safety

Autotalks

1 Executive Summary

V2X Road Side Units (RSUs) are becoming pillars of safety for vehicles of all levels of automation. Road infrastructure, equipped with V2X RSUs, enable safety-critical services, such as Traffic Light Status, Collective Perception, and In-Vehicle Signage.

The benefits to all road users are immediate and significant: information is distributed by the RSU to the surrounding vehicles equipped with V2X. The vehicles consume the received information and based on it may generate safety alerts to the driver or, in case of an automated vehicle, actuate braking. A prerequisite for the services is that the RSUs are a trusted source of information. The trust is achieved by a combination of cybersecurity oriented design and a path to Functional Safety.

The white paper analyzes for the first time the Functional Safety requirements of RSUs and addresses the specifics of cybersecurity protection.

2 Benefits of V2X RSUs for road users

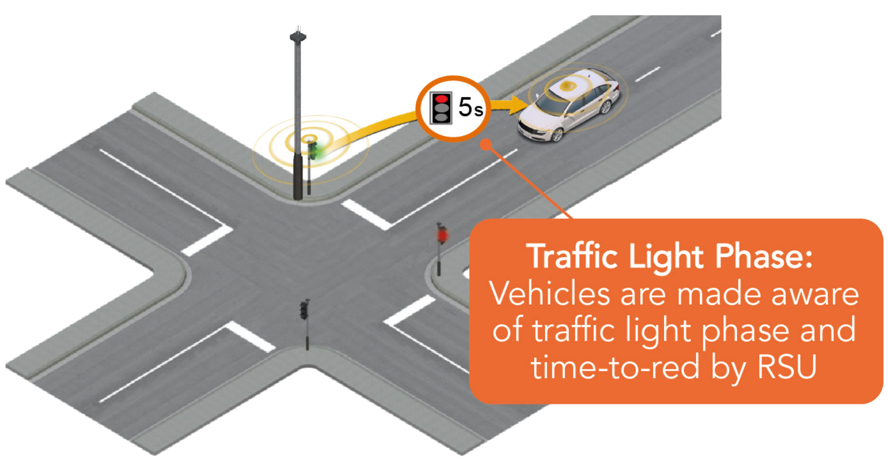
Driver experience in new cars today is significantly different from that of 15 years ago. A suite of sensors and advanced driver assistance systems warn us of situations such as lane departure and possible forward collision. The vehicle can autonomously keep the desired speed, and even take full control of the driving in some situations.

A vehicle's level of situational awareness is mostly achieved by line-of-sight sensors (camera, radar, lidar). The only sensor that can extend the vehicle's field of view beyond line-of-sight, and even share the intent of other road users, is V2X. All road-users equipped with a V2X sensor, including vehicles, RSUs, trucks, motorcycles, and, in the future, pedestrians, can securely exchange messages to indicate their location, speed, direction, and planned actions. More information about Functional Safety analysis of V2X applications can be found in [1], while in this article we will focus in detail on the interaction between the vehicles and road infrastructure.

We will illustrate the need for high levels of trust required from V2X RSU to enable secure messaging in several examples.

Example1: Traffic Light Phase

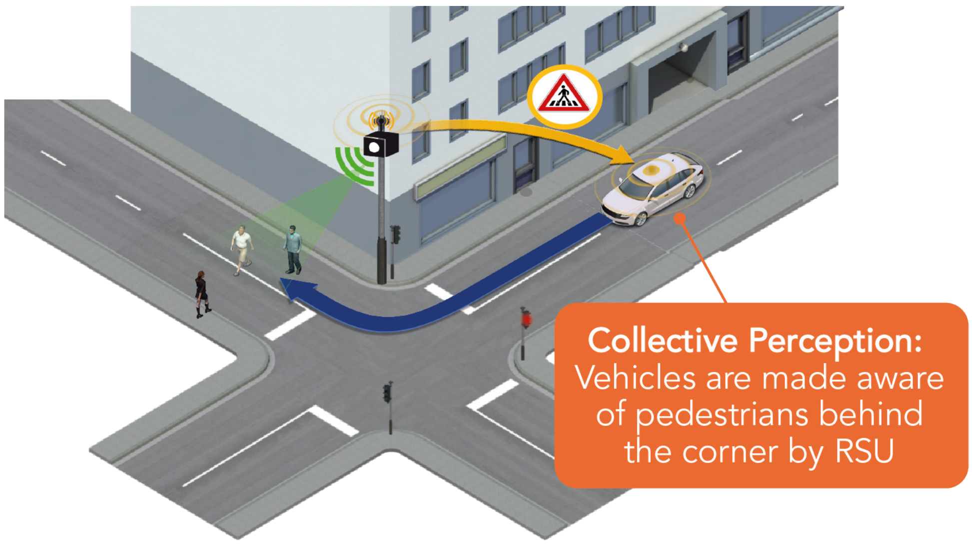
The vehicle receives SPaT (Signal Phase and Time) messages from the V2X RSU connected to the traffic light controller. The information contains both the current phase of the traffic light and the time to the next phase. Based on the received information, the vehicle driver assistance system recommends to the driver the ideal approaching speed. In the case of an AV, the vehicle will drive at the optimal approach speed. There may be malicious actors trying to falsify the traffic light status, or the signal may be wrong due to a malfunction. This could result in a wrong driver notification or in a failure to approach the intersection safely, potentially running a red light. The receiving vehicle must be able to identify possible cyber-attack, and for the RSU to identify its failure and stop transmission.



CAR 2 CAR Communication Consortium Illustration Toolkit
Scenario Developed by Autotalks

Example2: Collective Perception

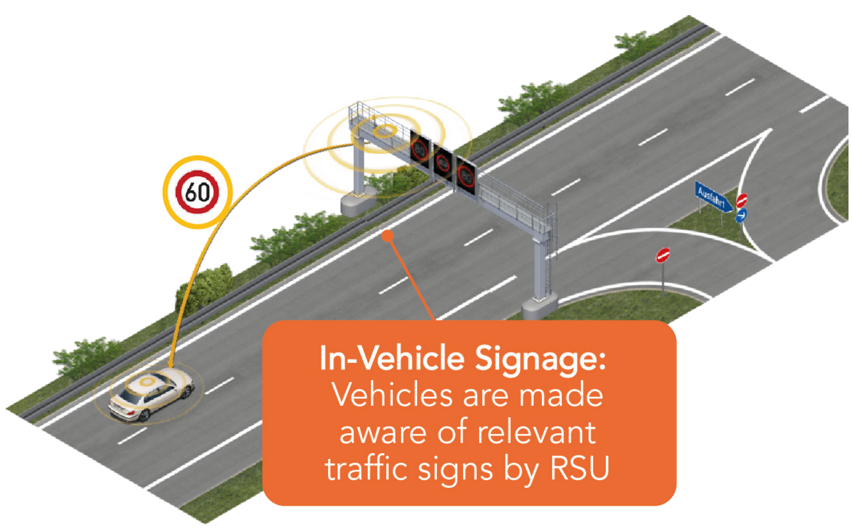
The vehicle receives objects detected by the V2X RSU equipped with a line-of-sight sensor, such as a camera and machine vision capability. The messages contain the locations of all detected pedestrians and other road users, potentially not detectable by the driver. Based on the received information, the vehicle's driver assistance system decides to warn the driver or start braking. In this example, sending false information to the vehicle by the RSU, whether due to cyber attack or malfunction, may cause the driver or AV to initiate braking without justification and create a road hazard.



CAR 2 CAR Communication Consortium Illustration Toolkit
Scenario Developed by Autotalks

Example3: In-Vehicle Signage

The vehicle receives IVI (In-Vehicle Information) messages from the V2X RSU. The messages contain information about existing, fixed, and dynamic traffic signs. Based on the received information, if the vehicle violates a safety-critical sign, the driver assistance system decides to inform the driver or, in the case of an AV, potentially trigger vehicle actuation. Also in this example, compromised content of the V2X message may cause the driver or the AV to initiate unwarranted braking and create a dangerous situation.



CAR 2 CAR Communication Consortium Illustration Toolkit
Scenario Developed by Autotalks

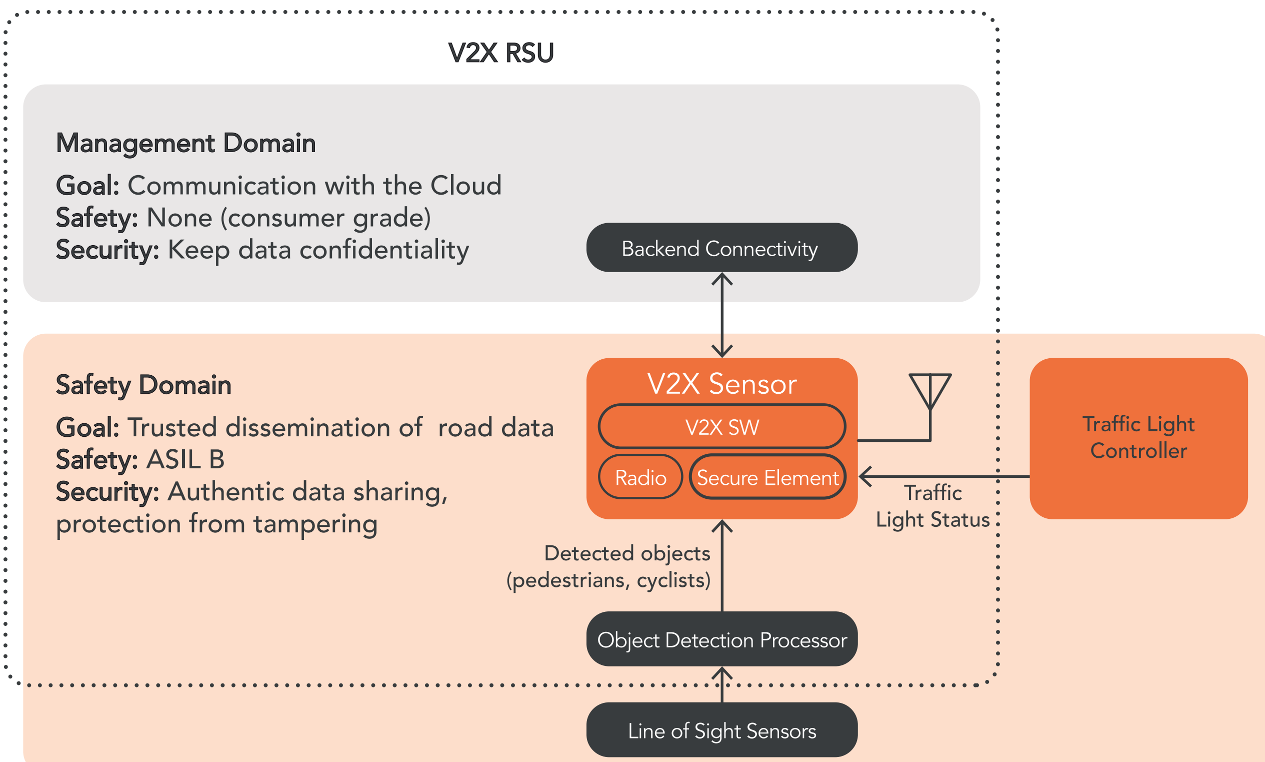
The technology brings a great promise of increased safety to all road users. The examples show that compromised data received by the vehicle, whether due to malicious activity or as a result of technical malfunction, can result in a wrong decision taken by the vehicle's driver or the AV and potentially endanger the passengers or others. There are design principles that will assure a high trust level of the shared V2X data and allow the receiving vehicle to rely on it as an input to its decision making. We will discuss in more detail the topic of trust and the design principles to achieve it in the next chapter.

3 Making a Trusted RSU

Inside V2X RSU, there are two functional domains, which have different potential safety impacts on the road users:

> The Safety Domain (see in the figure below) assures the dissemination of road safety data in a trusted way to the surrounding road users

> The Management Domain links the RSU to remote servers, such as a traffic management system.



Trust is the key in a distributed network of RSUs and vehicles, where the vehicles encounter the RSUs for the first time and rely on the information coming from it to alert the driver or actuate the vehicle brakes.

Design for Functional Safety

V2X sensor design flow for Functional Safety begins with an analysis of use cases, where system malfunctions can result in dangerous outcomes for the road users. As part of the analysis, ASIL goals are set for the main functions of the V2X sensor. In this paper, we refer to ASIL obtained in [1]. The reader is welcome to review the whitepaper in order to get a deeper explanation of use case analysis in the context of safety.
Main safety goals are listed here:

1. **Assure integrity of V2X messages (ASIL B):** V2X sensor will detect modified content of the V2X message. The possible reasons for content change include memory bit flips due to solar radiation, memory corruption, and malicious content manipulation by a 3rd party.

2. **Assure operating V2X link (ASIL A):** The V2X sensor will detect failures to transmit or receive V2X messages. These failures may result from ESD damage to RF components, electrical circuit damage due to environmental conditions, or a poorly mounted antenna after maintenance.

3. **Assure reliable data exchange between the V2X sensor and other RSU components (ASIL B):** The V2X sensor will detect corruption in the traffic controller data. Corruption can occur following physical damage to an electrical interface. Such damage can be a result of weather damage to the cable or electromagnetic interference (EMI).

4. **Assure correctness and integrity of software flow execution (ASIL B):** The V2X sensor will detect failures in its own SW execution. Software flow failure can occur due to reasons such as memory bit flips from solar radiation or an unhandled exception.

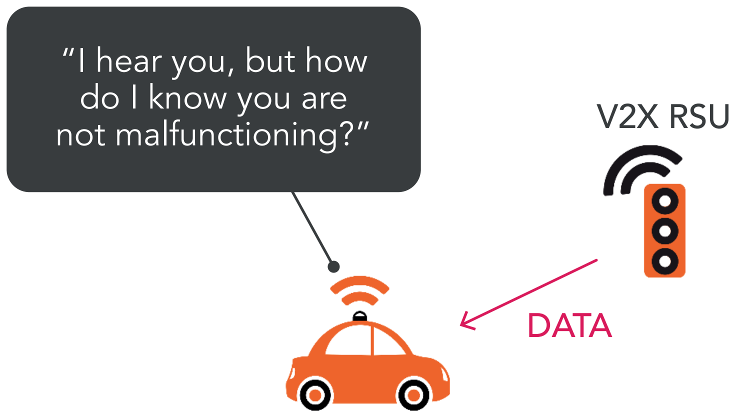
5. **Assure correct functionality of V2X security subsystem (ASIL A for signing):** The V2X sensor will detect failures in its security flows. Security flow failure can occur due to memory bit flips from solar radiation or EMI on electrical interferences between the discrete integrated circuits (ICs).

Any failure detection must occur in a defined short period, and the system must enter a defined safe state, in which the failure cannot pose a risk to the road users.

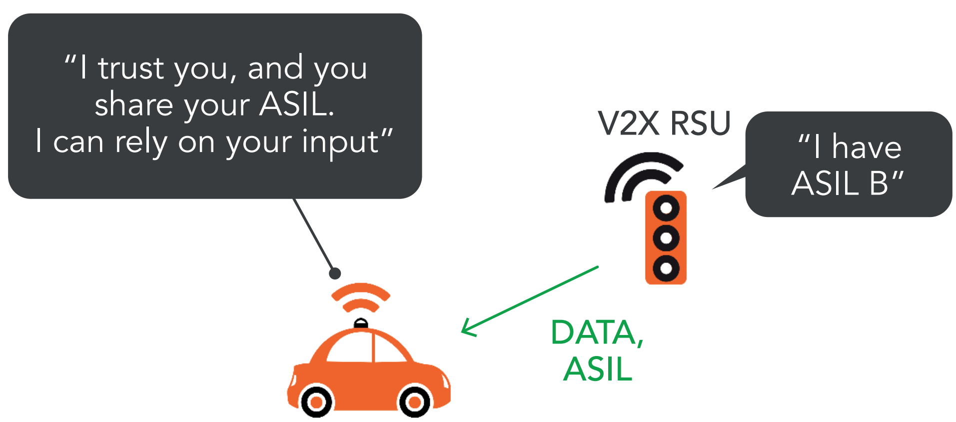
Subsequently, safety goals are translated into functional and technical safety concepts, which define requirements for products. After product hardware and software components are developed, the system undergoes validation.

Advertisement of safety capabilities[1]

Vehicle actuation decisions should be taken based on reliable input. The vehicle receiving safety-critical information from the RSU should know that the RSU will not introduce unreasonable risk due to a malfunction, by having the internal ability to detect all relevant failures and mitigate their impact.



The ASIL will be added to the V2X message by the sender and will provide the receiver with the knowledge of sender Functional Safety capabilities.



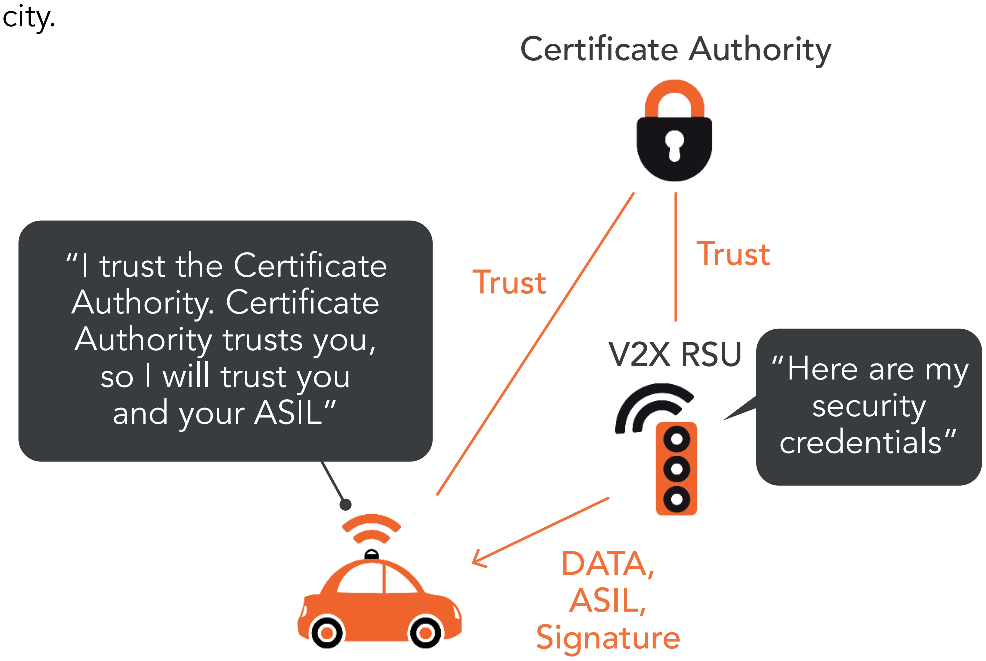
Upon reception of the V2X message, together with the ASIL, the receiver can assign a proper level of trust to the input, and decide which actions can be taken based on it.

1 All diagram's in this section are conceptual, the implementation is more nuanced

Assuring data authenticity

When a vehicle receives a message from an RSU, it needs to make sure the received information is from a source authorized to send this type of information.

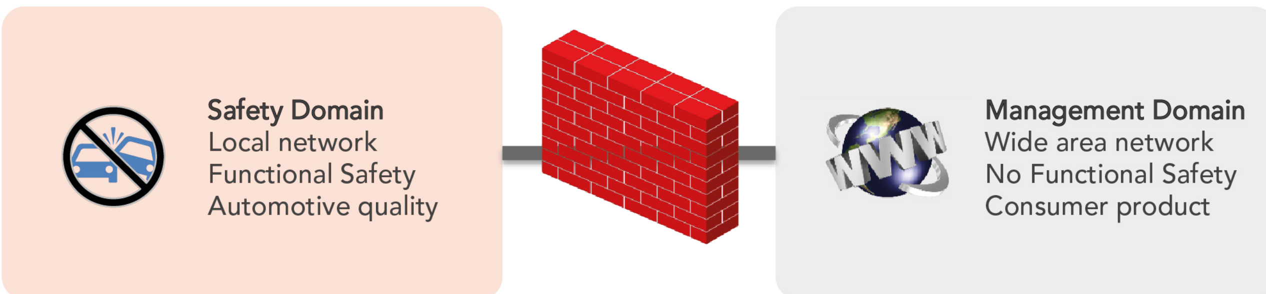
Each V2X message sent by the RSU is digitally signed by the Secure Element. Digital signatures are created uniquely for each message in such a way that it is impossible to change even a single bit in the message, without immediate detection of the change by the receiver. The digital signature contains the certificate of the RSU, signed by the Certificate Authority known to and trusted by the vehicle. Thus, the digital signature prevents message content manipulation and assures the receiving vehicle of RSU authenticity.



To make sure the digital signature mechanism is implemented following security requirements, and private keys of the RSU are protected, the RSU design has to be approved by the authority overseeing road equipment deployment. This approval typically mandates a formal certification by a 3rd party evaluator. An example of such a security requirement is the Protection Profile for V2X RSU and the Secure Element, and the requested process is Common Criteria security certification.

Domain Isolation

V2X RSU domains are exposed to different security threats. The Management Domain is used to access the public network and the Internet. It contains a complex, wide area network access device (e.g. a cellular modem which is usually a consumer-grade product used in mobile devices). The Safety Domain contains a V2X sensor - a short-range communication device communicating only with near-by vehicles on a dedicated frequency band. It has no access to the public network and is an automotive-grade product designed for safety applications.



To prevent a possible vulnerability in the Management Domain to serve as an attack point on the Safety Domain, strict isolation is recommended. Such isolation is typically achieved by a combination of physical isolation between elements, as well as clearly defined and well protected logical interfaces connecting the domains.

Another argument for physical isolation between domains is due to Functional Safety considerations. Management Domain would typically have QM ASIL, and to achieve target ASIL A/B in the Safety Domain, independent operation (i.e. failure in non-safe Management Domain will not impact Safety Domain) will need to be shown.

Summary

Road-Side Infrastructure is operating for a long duration after installation, and hence should consider future use cases. In this article we have explained that the RSU should target Functional Safety ASIL B level to allow a vehicle to actuate based on a received message, and should have certified HSM and domain isolation to be considered a trusted V2X source.

Want to Learn More?

[1] Functional Safety for vehicular V2X systems: https://www.auto-talks.com/technology/functional-safety

[2] C-Roads - largest RSU deployment initiative in EU: https://www.c-roads.eu/platform.html

[3] USDoT Security Credential Management System (SCMS) Technical Primer https://rosap.ntl.bts.gov/view/dot/43635