Functional Safety

for Enabling Present and Future V2X Use-Cases

Autotalks

Executive Summary

V2X provides unparalleled, precise and extensive data about all road users that transmit their detailed information. In the future, V2X will evolve to provide additional data about the objects detected by other vehicles' onboard sensors.

The primary goal of V2X is to save lives, which can be achieved by controlling vehicle movement in an emergency situation. Another important goal involving vehicle control is enhancing traffic efficiency by improving coordination with surrounding vehicles. V2X is expected to become a safety-critical sensor around the middle of the decade. As with other safety sensors, functional safety processes need to be implemented when V2X will influence vehicle control.

OEMs consider the requirements of future generations, thus the importance of the current discussion of functional safety for V2X. In addition, ADAS solutions are predicted to introduce upgradability over the vehicle lifetime, implying that current designs should already include functional safety V2X for future usage.

This paper describes the need for ASIL process for the V2X sensor by examining V2X use-cases and outlines the steps of implementing functional safety for the V2X sensor. The functional safety requirements are divided in two: integrity of operation should support ASIL B for minimizing false alarms, and operation of V2X link should support ASIL A for increasing V2X availability for mitigating accidents. The methods to achieve ASIL are described. The analysis is agnostic to the V2X protocol, whether it is C-V2X or DSRC, and the conclusion is that only a dedicated and meticulous V2X design can achieve the needed functional safety level.

Overview

Vehicle-to-everything (V2X) communication aims to dramatically improve traffic safety and efficiency. All road-users, including vehicles, trucks, motorcycles, and, in the future, pedestrians, securely exchange messages in order to indicate their location, speed, direction and other properties.

V2X applications will be launched in phases, known as "Day1", "Day2" and "Day3". Day1 V2X offers life-saving situational awareness. Day2 V2X applications can make use of sensor data shared by other vehicles. Day3 V2X applications primarily provide the means for negotiations between vehicles for increased road use efficiency and safety. Applications in all phases can influence vehicle movement, in an increasing number of road situations as phases advance.

An alert-only system does not require functional safety (ISO26262 QM is sufficient). In order to simplify the introduction of V2X, early Day1 implementations only alert the driver, without controlling the vehicle. Only when the V2X system will influence vehicle movement, the true value of V2X will be unlocked.

Any vehicle control circuitry should be analyzed for potential malfunctions that may risk lives. Functional safety process assures that risks are mitigated. Functional safety analysis begins by setting the safety goal resulted from Hazard and Risk Analysis (HARA). The safety goals are classified as Automotive Safety Integrity Levels (ASIL A, B, C or D) according to ISO 26262 functional safety standard. Hazards are evaluated and classified according to their potential severity, exposure and controllability:

> Severity: level of injury from S0 (no injuries) to S3 (fatal injuries)
> Exposure: probability of the risk scenario from E0 (incredibility unlikely) to E4 (high probability)
> Controllability: driver's ability to prevent injury from C0 (controllable) to C3 (uncontrollable)

Safety-capable V2X is not a Futuristic Requirement

The hazard analysis and ASIL assigned have no dependency on V2X penetration. A failure in V2X operation, potentially risking lives, occurs regardless of the presence of other vehicles with V2X. Our model assumes mass-scale deployment of V2X. A vehicle designed today will only be launched in 3 years' time, sold for an additional seven years and will likely carry passengers for up to 15 years.

V2X influence on vehicle control will grow over time. An increasing number of OEMs will use Over-The-Air (OTA) software updates to update ADAS and other vehicle systems throughout the vehicle's lifecycle. Following a software upgrade, existing hardware may run new and advanced safety applications. The hardware should have sufficient capacity to handle that, mainly security and CPU power, but also its functional safety grade should match future needs.

V2X Use-Cases

Decreasing speed, based on V2X data, can prevent or significantly reduce a severity of the possible accident

Vehicles located a few hundred meters apart can communicate using V2X. A dangerous situation can be detected very early on, long before the driver or other driving assistance sensors can observe the danger. Consequently, the reaction to such alerts can be well thought out and relaxed. In most cases, there is no need for hard braking or rapid manoeuvring, since there is sufficient time to slow down and mildly change the course of the vehicle to avoid the danger. Without bounding the deceleration, false V2X operation should have defined higher grade ASIL than B.

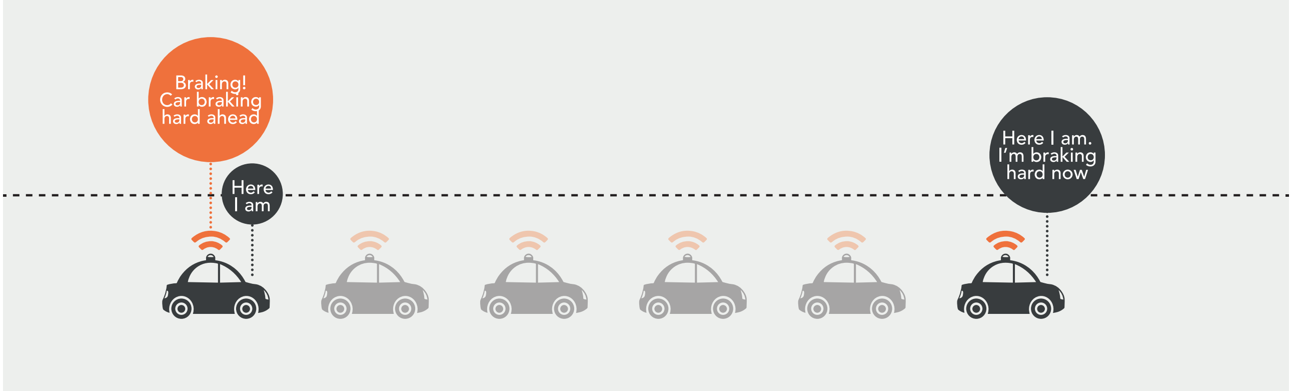
Day1 Safety Use-Cases

Day1 applications use information from the vehicle sensors, and indications from smart intersection roadside units[1]. Day1 applications can be used to influence the control of the vehicle to prevent an accident.

Emergency Electric Brake Light (EEBL)

Use-Case Description

Day 1 – Driving Awareness
Use case – Emergency Electric Brake Light


Braking! Car braking hard ahead
Here I am
Here I am. I'm braking hard now

An example of V2X early detection capability is when a vehicle ahead brakes abruptly due to driver error or road hazard. Unalerted drivers behind this vehicle may respond too late and have to brake hard to prevent an accident. This can create a chain-reaction, impacting more and more vehicles behind the incident. Without V2X, the driver will notice the braking only when the vehicle right ahead is forced to brake and its brake lights shine red. With V2X, the vehicle's ADAS detects the event well in advance, and can moderately decelerate, increasing the gap from the vehicle ahead, thus avoiding hard braking. Still, the deceleration limit should be set sufficiently high to prevent urgent emergency braking.

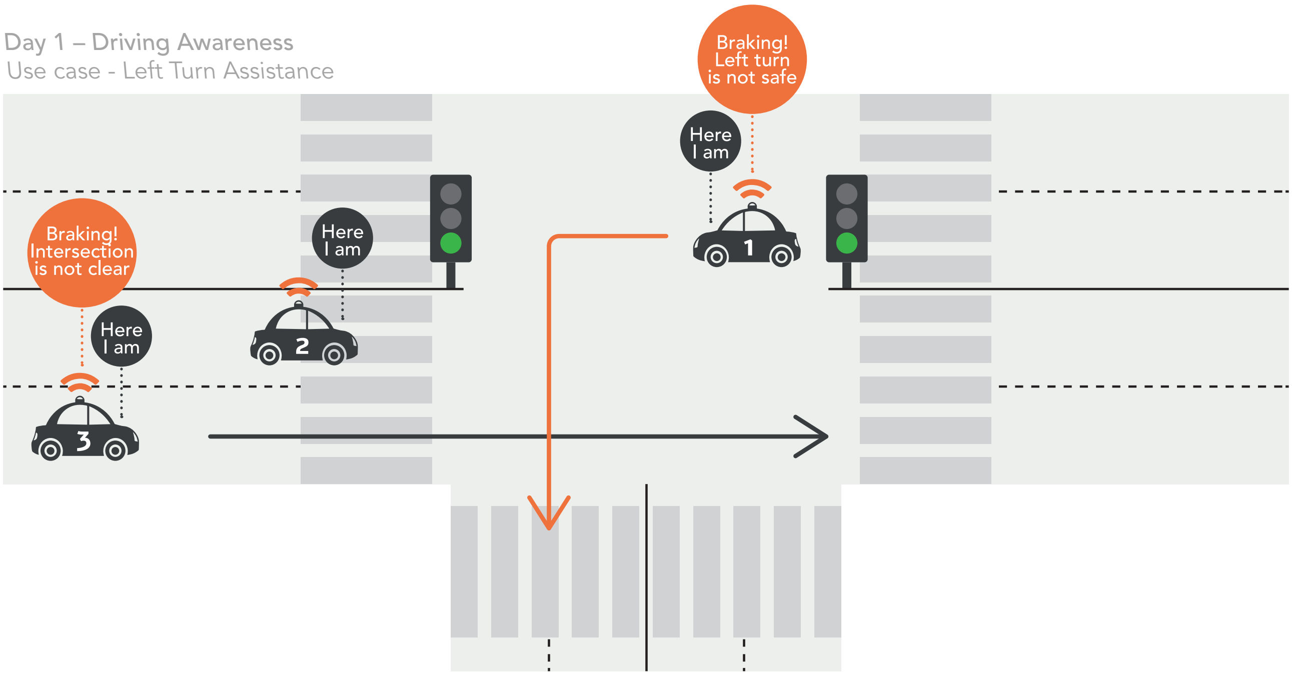
[1] A smart intersection roadside unit typically has onboard vision sensors, V2X and processing capabilities. It is capable of sharing detected objects, such as crossing pedestrians, with road users via V2X messages.

Use-Case Analysis

A false event could have a serious impact as an unexpected braking on a highway is dangerous to the ego vehicle and to the vehicles behind it. Controllability is simple (C1), severity is life-threatening (S3) and probability is high (E4), leading to ASIL B for avoiding a false alarm. The false alarm mitigation sets reliability and integrity requirements for both the receiving vehicle and the transmitting vehicle. The transmitting vehicle should not transmit messages that can risk another vehicle, and the receiving vehicle should not risk itself by misinterpreting received messages.

Left Turn Assistance

Use-Case Description



Day 1 – Driving Awareness
Use case - Left Turn Assistance

Braking! Intersection is not clear
Here I am
3
Here I am
2
Braking! Left turn is not safe
Here I am
1

In some right-hand traffic countries, traffic lights allow driving straight and turning left concurrently in both opposing lanes. Left turning vehicles have to patiently wait until the turn can be completed safely. Even in perfect visibility, upcoming vehicles can be obscured. For example, a vehicle planning to turn left (#2) is hiding the view of vehicles approaching straight (#3) from the vehicle planning to turn left (#1) in the opposite lane.

Use-Case Analysis

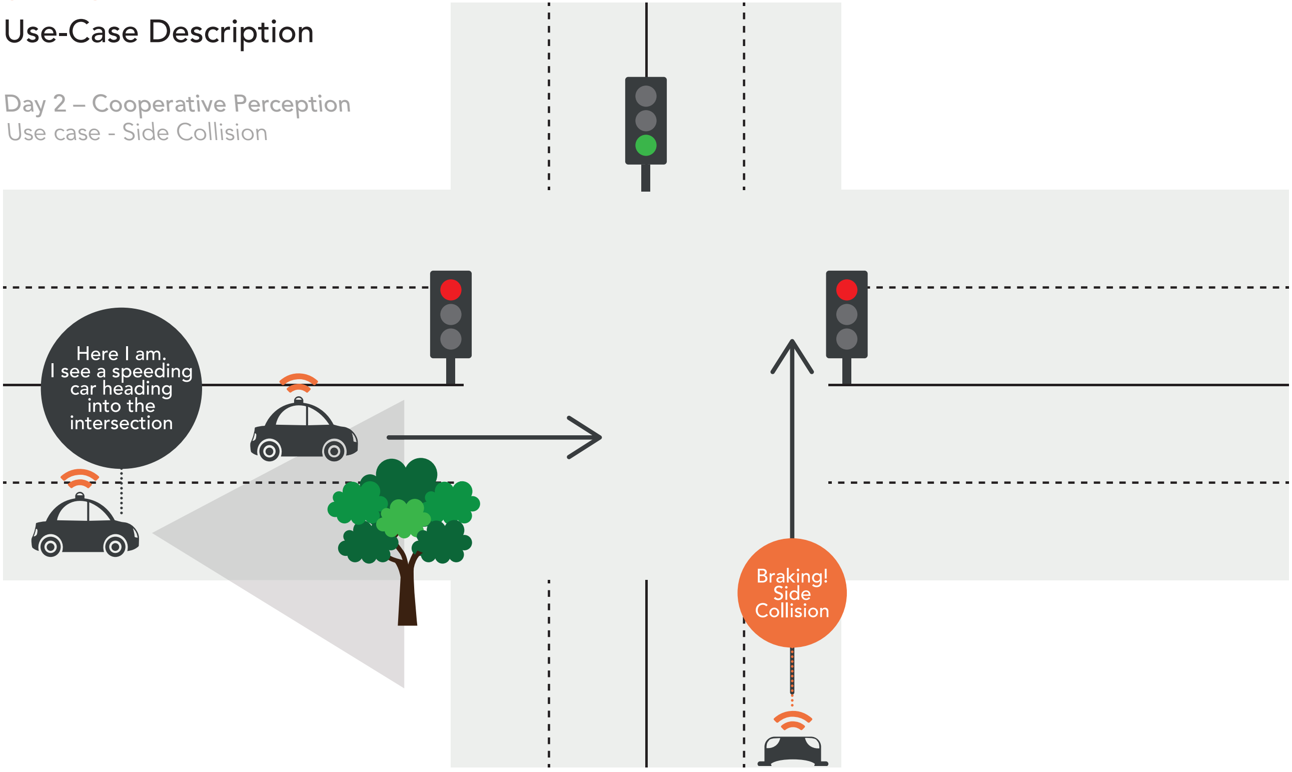
Analysis of V2X failure, according to ISO26262, is limited to the difference between the severity of an accident without V2X influence and the severity of an accident with V2X influence. V2X is the only sensor that can alert both vehicles' ADAS, the one continuing straight and the one turning left, from an imminent accident. The hazard is life-threatening (S3) since the vehicle continuing straight approaches at a high-speed and risks crashing into the side of the vehicle turning left, the controllability is uncontrollable (C3) as assumed for an accident situation, and probability is very low (E1) assuming accidents occur less often than once a year. This analysis leads to ASIL A for transmit and receive functions of both vehicles, or in other words, for the V2X link between the two vehicles.

Day2 Safety Use-Cases

As mentioned before, Day2 applications are using information of sensors shared by other vehicles. A second V2X radio channel is needed to communicate the sensor information. Day2 implementations are assumed to trigger control of the vehicle.

Side Collision

Use-Case Description



Day 2 – Cooperative Perception
Use case - Side Collision

Many intersections, especially in urban environments, have limited visibility. Accidents commonly occur due to right-of-way violation. With V2X, an ego vehicle's ADAS is alerted when another vehicle is heading into the intersection without an intention or possibility to stop even before it is observed by onboard vehicle sensors, such as camera and radar. The alerted vehicle is expected to nearly-hard brake (up to -3.5 m/s2). Soon after, the onboard vehicle sensors will be able to observe the violating vehicle entering the field of view, and a hard brake may be decided upon.

If the vehicle bursting into the intersection is equipped with V2X, it will report its own trajectory. Alternatively, it may be reported by other vehicles with V2X. The functional safety analysis does not depend on the source of the report.

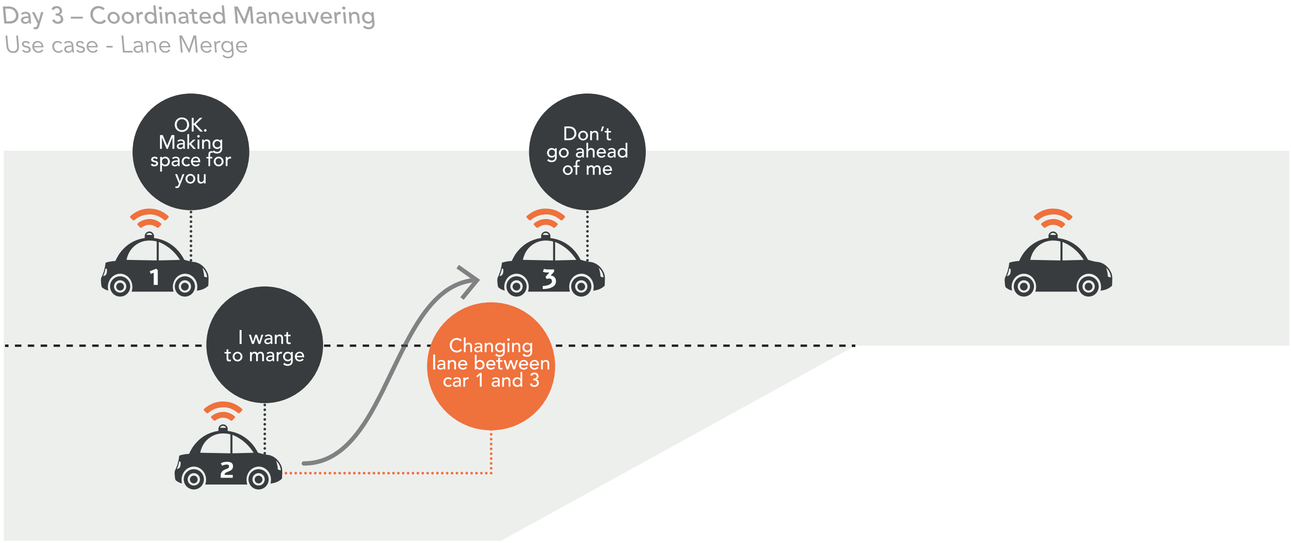
Use-Case Analysis

The risk due to false alert is considerable since braking is nearly-hard. A vehicle may stop without justification in the middle of an intersection. That risks the vehicle, other vehicles behind it, and other vehicles which may be inside the intersection. The hazard is life threatening (S3), controllability is medium (C1), and exposure is high (E4) leading to ASIL B of message integrity functions. Similarly to the mis-activation of V2X in Left-Turn-Assistance case, the hazard of missing the offending vehicle is life threatening (S3), the controllability is uncontrollable (C3), and probability is very low (E1). That leads to ASIL A for V2X link functions.

Day3 Safety Use-Cases

Highway lane marge coordination

Use-Case Description



Automated highway merge can improve traffic efficiency. Highway traffic would flow better and safer as vehicles would merge in an organized manner without impacting other vehicles' speeds.

Using the vehicle's turning signal is just one method to negotiate right-of-way, and not necessarily the most effective one, as drivers may use eye contact (or lack thereof), slow down to show willingness to give right-of-way or non-verbal gestures. These negotiation methods are unavailable for automated vehicles (AVs), which are expected togain popularity by the end of the decade.

Use-Case Analysis

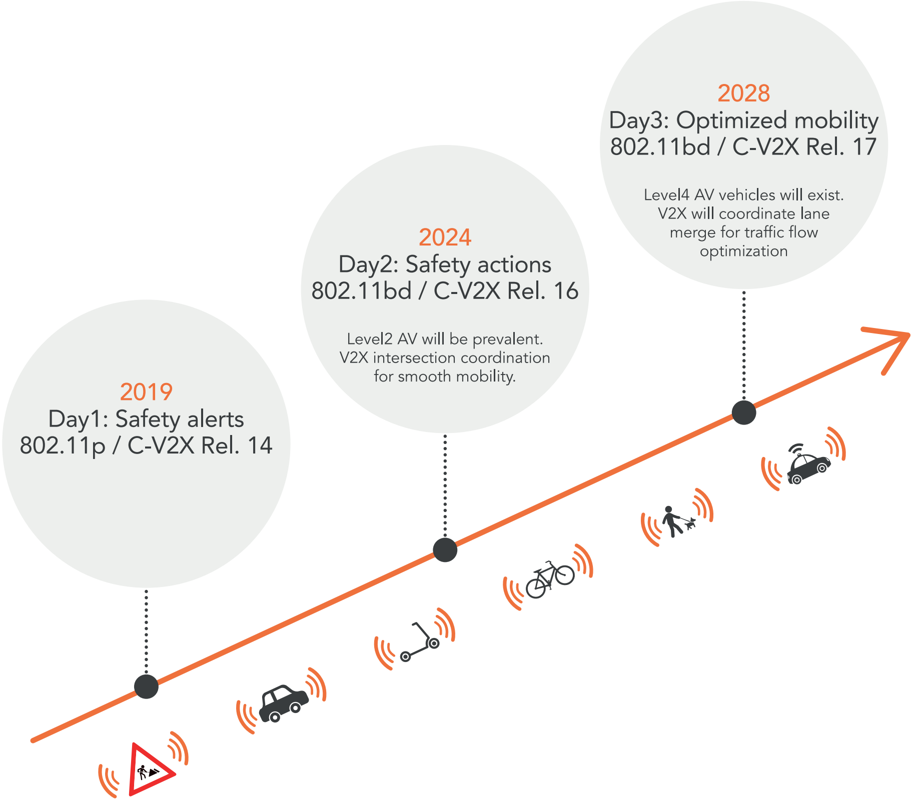
The risk of two vehicles mistakenly reaching the same point at the same time due to V2X failure is extremely high. The severity is life-threatening (S3), the controllability is difficult (C3) since the path negotiation failed, and one vehicle does not know the planned path of the other vehicle, and probability is high (E4), leading to ASIL D. That does not imply that the V2X sensor should be ASIL D, but it does imply that the composition of the V2X system, which may include two V2X sensors, should reach ASIL D.

V2X Roadmap Timeline

Moving from one V2X deployment phase to the next, such as from Day1 to Day2, is conditioned by multiple factors:

> Availability of next generation communication standards: Day2 use-cases require the reliability and highest level of communication throughput , hence the latest and most advanced communication standards should be preferred: 3GPP C-V2X Rel. 16 or IEEE 802.11bd. These standards are being concluded, and commercialization of products will happen in a few years' time.
> Automated vehicle penetration: AVs will operate more reliably with V2X, in particular for reliable object detection with rich data, traffic light indication, coordination between road-users and ability to detect obstructing objects. The greater the penetration of highly Automated Vehicles, the higher the need for V2X Day2 / Day3 deployment.
> Regulation and spectrum availability are also major factors, but are outside the scope of this paper.

Market expectations are outlined below. Day1 services are mass-deployed from 2019, deployment of Day2 services is planned to commence in late 2024, and Day3 is expected to follow in 2028, once the need for AV coordination will increase.



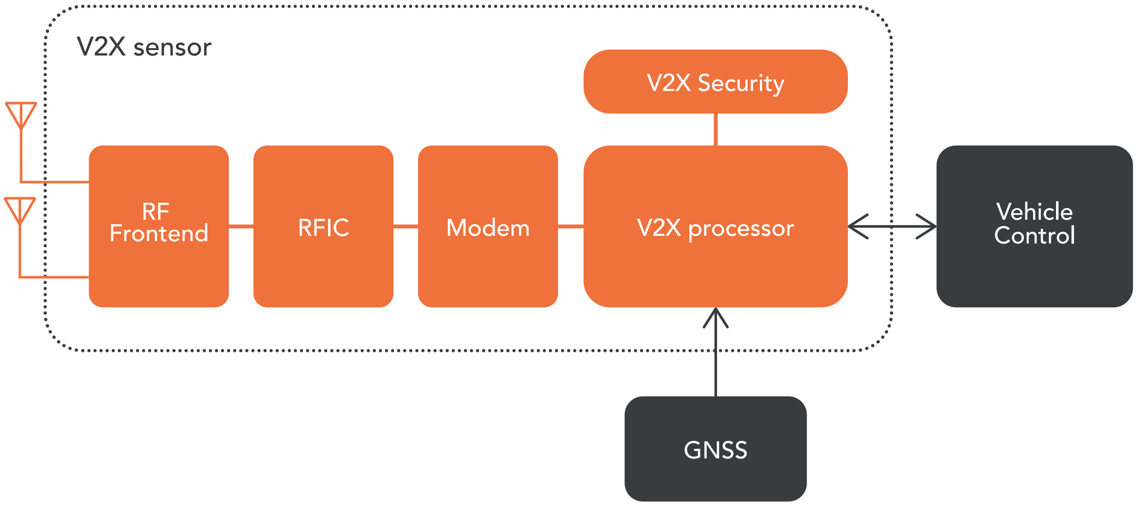
Functional Safety in V2X Sensor Design

The conclusion from the above analysis of V2X use-cases, is that V2X operation integrity should achieve ASIL B, and V2X communication link functions should follow ASIL A in order to unlock its life-saving potential in common Day1 and Day2 safety use-cases. Day3 use-cases require system level ASIL D operation.

Automotive industry practice is that systems, in which a malfunction may endanger human lives, should be analyzed in the context of Functional Safety.

A high-level block diagram of a V2X sensor is shown below. The V2X sensor includes wireless interface for communicating with other V2X-enabled devices, in-vehicle communication interface with other vehicle control units, and positioning interface to high precision automotive GNSS receiver.

Figure 1: High level diagram, depicting V2X sensor, including processing, security and communication subsystems



The entire system is subject to functional safety certification. Failure In Time (FIT), defining the number of failures that can be expected in one billion (1x10^9) device-hours of operation, should be less than 100 for ASIL B system. In other words, a device is expected to operate continuously 1,141 years without an undetected failure. Failures are accumulated over all V2X sensor subcomponents, including the memory and power supply. The latter components may contribute 50 FIT, thus leaving only 50 FIT for the V2X chip.

FIT is calculated using a mathematical model defined in IEC 62380. This FIT rate depends on technology, package and application conditions (mission profile). A few contributing points are:

> Mission profile: Operating temperature has a significant impact on FIT. The ambient temperature of V2X is rather high to begin with since the device is commonly located on the roof of the vehicle, close to the antennas. A V2X device that handles additional non-V2X functionality, like cellular connectivity, will heat-up more easily. Furthermore, the V2X/cellular combo devices tend to have a smaller package, and to be placed very close to additional components, which generates more heat.

> Process reliability: Automotive IC physical design follows strict design rule checks (DRCs). These lower the FIT compared with consumer grade devices.
> Silicon area: FIT is proportional to the chip area that is susceptible to a critical failure. A dedicated V2X design shrinks this area, compared to a generic device which combines V2X with additional functionality.

How can Functional Safety be Achieved?

Applying Functional Safety to a V2X sensor is a novel process.

The flow begins with an analysis of use cases, where V2X sensor malfunctions can result in dangerous outcomes for road users. The next step defines safety goals of the V2X sensor for risk mitigation.

The main safety goals proposed for the V2X sensor are:
> Assure integrity of V2X messages (ASIL B)
> Assure operating V2X link (ASIL A)
> Assure reliable data exchange between the V2X sensor and other vehicle subsystems and positioning (ASIL B)
> Assure correctness and integrity of software flow execution (ASIL B)
> Assure correct functionality of V2X security subsystem (ASIL A for signing, and ASIL B for verification)

A failure causing a violation of the above goals shall be detected within a short time, and the system shall transition to a safe state. Examples of failures resulting in violation of the above goals:

> V2X integrity (ASIL B): Software flow execution can corrupt the outgoing message or badly process the received message and security verification can allow corrupt message due to reasons such as memory bit flips from sun radiation or source clock jitter
> V2X integrity (ASIL B): V2X sensor data link to other vehicle subsystems may receive corrupted data following physical damage to vehicle internal harness
> V2X link (ASIL A): V2X transceiver may fail due to physical or electrical damage to RF periphery, such as following bad antenna assembly or ESD
> Normal V2X operation (QM – no safety measures): V2X message integrity can be compromised by noise in the wireless channel. This is detected using inconsistent 802.11 CRC or V2X 256-bit message signature

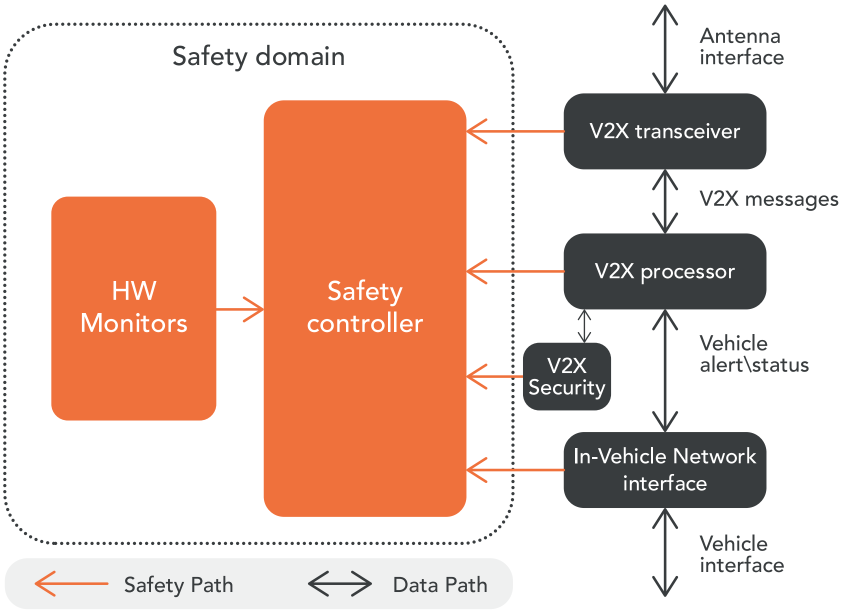
Subsequently, safety goals are translated into functional and technical safety concepts, which define requirements for products. After product hardware and software components are developed, the system undergoes validation.

V2X Sensor Safety Architecture

Safety concept requirements result in adding dedicated hardware and software mechanisms to the V2X sensor. The main objective of the safety architecture is to ensure sufficient resilience to failures, detecting them in a timely manner and transitioning to a well-defined safe state.

V2X sensor safety architecture is shown in the diagram below:

Figure 2: High level diagram showing functional safety domain within V2X sensor

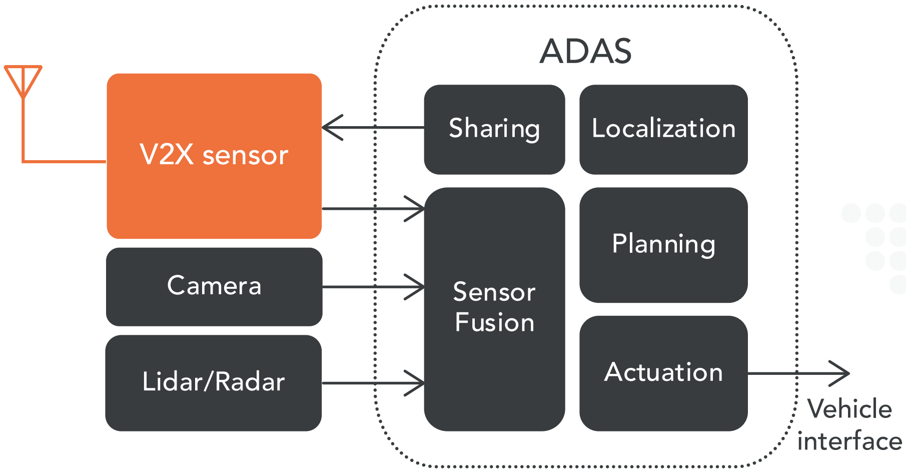


The safety domain is continuously monitoring the operation of the V2X transceiver, processor and in-vehicle network interface, in addition to IC integrity.

System Level Functional Safety

In order to provide a complete overview, the scope of discussion is extended to the ADAS level. Modern driver assistance systems are comprised of several sensors, feeding data to the vehicle ADAS control unit, which controls vehicle movement (see below).

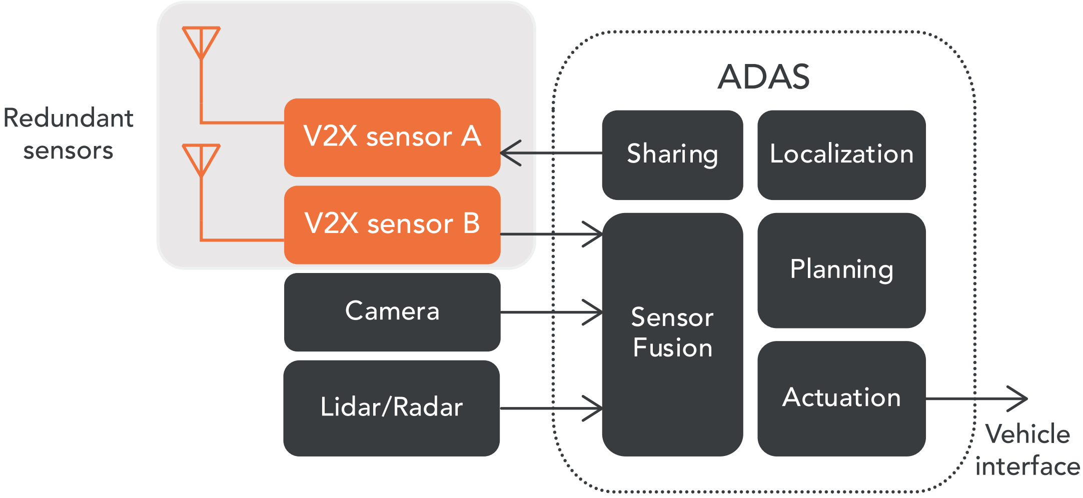
Figure 3: V2X sensor in ADAS context



While each sensor may achieve only ASIL B, the combination of sensors can reach ASIL D, which is the highest-level of safety integrity.

As explained above, cooperative merging may require ASIL D for V2X functionality since a failure is extremely dangerous.

Figure 4: Redundant V2X sensors in ADAS context



Safety Domain Isolation in Telematics

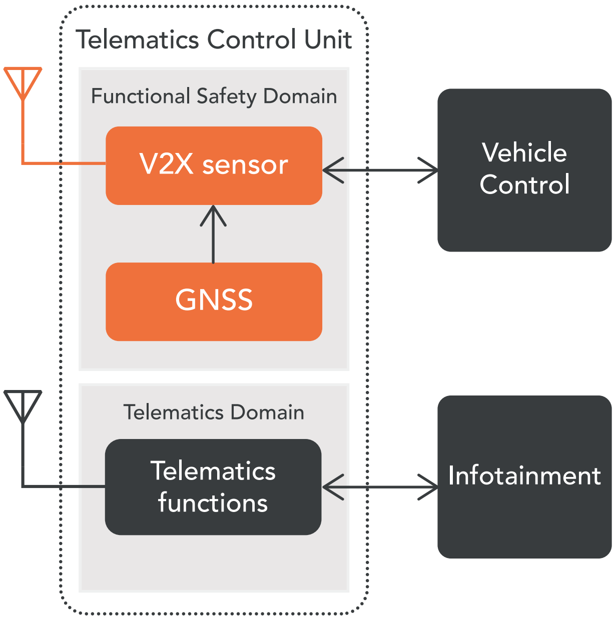
V2X is commonly placed in Telematics units, where both safety and non-safety functions are handled.

GNSS receiver is a critical source of positioning and timing information in the context of functional safety analysis. GNSS receivers, designed for safety critical applications, are already appearing in the market[2]. Such receivers, capable of ASIL B, are added as standalone devices by Tier1s when ASIL positioning is needed. These GNSS receivers are standalone devices since, so far, when integrated in other devices, they did not meet the required safety goals.

[2] Example of such a GNSS device: https://www.st.com/en/automotive-infotainment-and-telematics/sta9100mga.html

For the same reasons, designers of telematics platforms, with functional safety requirements or roadmaps, should consider isolating the V2X sensor from other functions, as shown in the figure below:

Figure 5: Telematics Control Unit Domains



Functional Safety Development Flow

The functional safety development flow is applied to all devices composing the V2X sensor, which could be combined into a single integrated device. The V2X device would have to undergo:

> Selection of functionally safe building blocks, including the processor running the V2X stack, analog elements, PHY, MAC and security
> Systematic failure analysis, considering all elements potentially impacting V2X operation, as well as their interaction paths, for identifying potential failure modes and their causes and effects
> Addition of protection mechanisms, like memory ECC
> Addition of fault detections, like SoC interconnect integrity
> Hardening device operation, for example lock-step V2X CPU, or running Software Test Library (STL), carefully designed to achieve target error detection coverage
> Quantitative analysis with FIT calculation

This is quite a challenging task. The larger the silicon device or the greater its functionality, the harder it is to successfully conclude the ASIL process, if at all feasible. Using certified devices significantly lowers the burden of achieving system level ASIL from the system owner.

Summary

V2X is expected to influence vehicle actuation in order to avoid accidents and improve mobility. It will mandate functional safety processes. Future and current vehicle architectures should be designed with this in mind.

V2X use-cases, even from Day1, should achieve ASIL B for V2X integrity and ASIL A for V2X link operation for detecting and mitigating life-threatening failures.

Only a dedicated and meticulous design can achieve the needed functional safety level.

References

[1] ISO International Standard 26262 "Road vehicles — Functional safety", Rev. December 2018

[2] SAE J2980: Consideration for ISO 26262 ASIL Hazard Classification

[3] SAE J2945/X family of standards for DSRC

[4] SAE J3161/X family of standards for C-V2X

[5] Nilsson, J., Bergenhem, C., Jacobson, J., Johansson, R. and Vinter, J. (2013), "Functional Safety for Cooperative Systems", SAE World Congress & Exhibition, Detroit, MI, USA, SAE International. https://doi.org/10.4271/2013-01-0197

[6] Eriksson, H. and Söderberg, A. "Remote Sensing and Functional Safety in ITS" In Proceedings of 12th ITS European Congress, 2017

[7] VW V2X deployment: https://www.volkswagenag.com/en/news/2018/02/volkswagen_group_rapid_road_safety.html

Abbreviations

ADAS - Advanced Driver Assistance System

ASIL - Automotive Safety Integrity Level

AV - Autonomous Vehicle

CAN - Controller Area Network

ECU - Electronic Control Unit

HARA - Hazard Analysis and Risk Assessment

LoS - Line of Sight

NLoS - Non-Line of Sight

QM - Quality Management

SOP - Start of Production

V2X - Vehicle to Everything

Functional Safety

for Enabling Present and Future V2X Use-Cases