TND6233/D
Rev. 1, MAY – 2018

Evaluating Functional Safety in Automotive Image Sensors

May, 2018 – Rev. 1
Publication Order Number:
TND6233/D

ON Semiconductor®

Evaluating Functional Safety in Automotive Image Sensors

Abstract

Almost all Advanced Driver Assistance Systems (ADAS) both today and in the foreseeable future are built primarily on machine vision to drive the decision process. With the rapid proliferation of ADAS solutions and the introduction of the ISO 26262 safety standard for passenger vehicles, functional safety considerations for those imaging systems becomes paramount. The manner in which safety measures are implemented and verified can have significant impact to the overall system design including cost, reliability, and complexity. This paper will examine functional safety in the imaging subsystem and its implications to system design.

Introduction

The first rear view cameras appeared in vehicles as early as 1991, primarily as an aid to safe reversing. In 2004, ON Semiconductor introduced the first CMOS sensor for automotive applications. In the United States the National Highway Transportation Safety Administration (NHTSA) mandated that by May 2018, all new passenger vehicles are required to include back-up cameras. Auto makers are now incorporating increasing levels of autonomy to further improve vehicle safety. As ADAS features like lane keeping assist, adaptive cruise control, and automated braking for collision avoidance evolve into true autonomy, additional cameras are making their way into production vehicles. The primary sensor in almost all ADAS systems is the image sensor. As ADAS systems progress from assistance to automation, the safe operation of the vehicle will depend more and more on the reliability of the imaging subsystem.

Underlying this trend is the fact that to ensure a level of safety in ADAS and autonomous systems, the image sensor becomes a critical component in the system's overall functional safety. With the introduction of ISO 26262, the concept of automotive safety integrity levels has been defined. ASIL levels range from the lowest, ASIL−A (lowest), to ASIL−D (highest). An ASIL level is determined by three factors, severity of a failure, the probability of a failure occurring, and the ability for the effect of the failure to be controlled. This paper will explore the issue of functional safety as it relates to the image sensor as well as to examine failure modes and safety

mechanisms that can be implemented to detect, protect, and/or correct image sensor failures. The key metrics that affect the safety performance of the system include detection, delay, efficiency, and effect.

Faults in semiconductor devices arise from a number of causes including cosmic radiation, electromigration, early mortality, and a host of other reasons. It is not the objective of this paper to examine the causes of faults in image sensors, rather it will be to examine the nature of faults, methods of fault detection i.e. safety mechanisms, and the effectiveness of those mechanisms. Here we will also discuss some factors that differentiate fault coverage claims and methodologies.

Functional Safety

To implement functional safety in an ADAS system requires that the system prevent or mitigate any action or behavior that could cause harm. The assessment of the probability of harm and the severity of that harm caused by a failure in the system allows system designer to classify levels of risk the system and to take appropriate measures to minimize the risk.

Often this requires fundamental changes not only in the development process, but also in the corporate safety culture ranging from organization structure to safety roles/officers and safety documentation, manuals, and standards. Responsibility for functional safety compliance in a system involves not only the ADAS supplier, but the entire supply chain from OEM to ADAS supplier to component providers. For robust functional safety, all key safety relevant components in the system must contribute to the overall functional safety, specifically, that safety starts at the source.

In order to minimize the risk caused by a particular failure, the system designers must, of course, identify possible failure modes that could affect the safety of the vehicle and determine an appropriate action to mitigate the risk. A key part of this process is the identification of all components that could impact the safe operation of the system. For each such component, an analysis of every possible failure mode must be made to determine whether a given failure mode might contribute to a failure in the system. Once the failure modes have been identified, mechanisms can be implemented to detect, correct, and/or protect the system from, a given failure.

The specific implementation of safety mechanisms for a given system has a tremendous impact on the cost, reliability and complexity of the solution, as well as its effectiveness at mitigating the risks to the system. Various levels of safety mechanisms can be implemented that range from simple fault detection and reporting, to mechanisms that protect from the occurrence of faults all the way to actually correcting a fault that has already occurred. A careful and balanced selection of system components can contribute to a more optimized and efficient implementation.

In order to further consider the concept of functional safety, a definition of failure must be made. In the case of ADAS, we can generally accept that a failure is any condition that causes the system to make an incorrect or even less than optimal decision. Examples of undesired decisions include late braking, over-steering, false object identification, or unintended acceleration.

Image Sensors and the ADAS Application

Image sensors are a core component of an ADAS system and the primary source of all vision system data. They provide the raw data which the rest of the system uses to analyze the environment and then make operational decisions in the vehicle. In effect, image sensors are the eyes of the autonomous vehicle. Other sensors like radar and lidar may also be used, but the primary source of data are the image sensors. In addition to the sensors, other components in the ADAS system include components that perform the functions of image processing, analysis and decision making.

As stated previously, the number of image sensors in a typical ADAS system is rapidly growing. From a single forward looking camera, to full surround view systems, the number of cameras in a vehicle can be anywhere from one (1) to over ten (10). The effect of failures in the sensor depend on the nature of the failure and can range from insignificant to critical. The ability for a system to detect, protect and correct individual failures in the image sensor have significant ramifications to the overall safety and reliability of the system.

At its core, a CMOS image sensor is a rectangular array of photo-sensitive pixels organized in rows and columns. These pixels convert the incident light into voltage or current with a per-pixel analog circuit. The current/voltage is then converted into digital values, typically in a row-by-row order. Additional digital logic enables the data to be stored, processed, and transmitted to other devices in the system for subsequent processing and analysis.

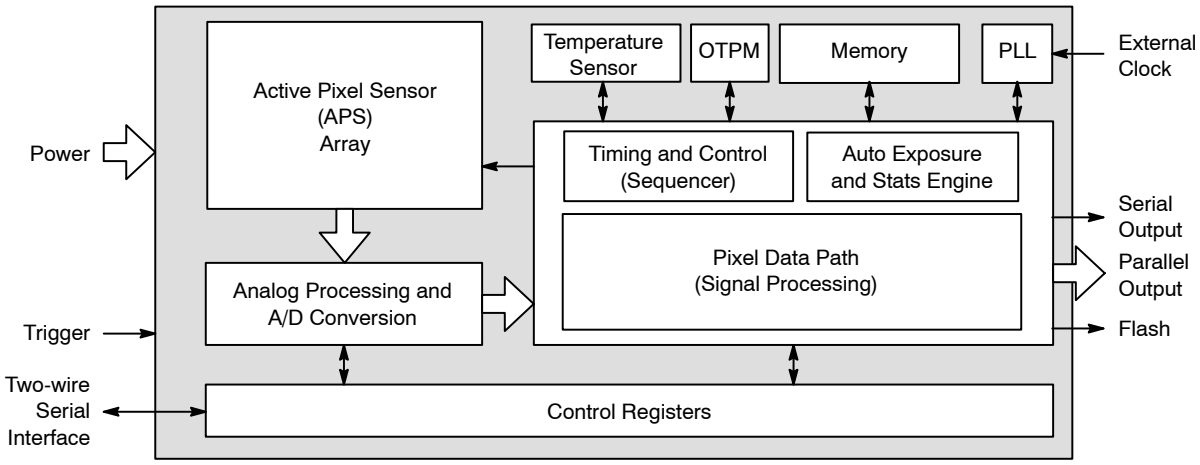

Figure 1. Block Diagram of a Typical Image Sensor

The data captured by the image sensor in an ADAS application is typically used by the system to make decisions that affect the operation of the vehicle. As ADAS systems have increased in complexity, these decisions have advanced from generating simple audible and visual warnings, to much more complex decisions including braking, acceleration and steering, and in the future will progress to completely autonomous driving. These advances in autonomous and semi-autonomous vehicles places increasing reliance on the image sensor and it safe operation.

Failures in Imaging Applications

A very conservative view of a failure in an image sensor would be to define an unsafe fault as any output that differs from a “fault-free” model or known-good device output as shown by the diagram below. At a granular level, this would imply that errors even at the pixel level could constitute a failure. At higher levels, row, column and frame errors could also constitute a failure. Implied are any problems in the internal operation of the device, either analog or digital, that could manifest themselves as pixel, row, column, or frame errors. Finally, errors in the physical transmission of data from the sensor to the rest of the system present another potential cause for failure. Due to the dynamic nature of video, faults can be both static, i.e. permanent or fixed, and dynamic, both spatially and temporally.

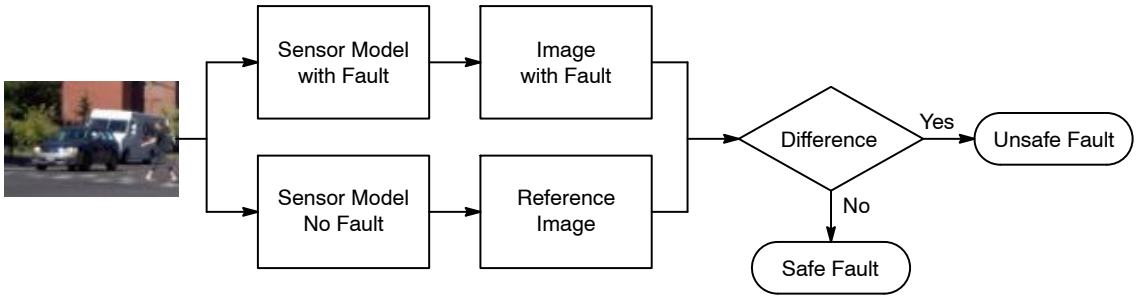

Figure 2. Flowchart to Determine Safe vs. Unsafe Faults

Taking this conservative definition of failure in an image sensor, the challenge to the system design is the detection of the presence of a failure. Additionally, the system may take measures to protect against the occurrence of a system failure or to correct or take corrective action in the presence of an individual sensor error. To better understand the implications to system level safety mechanisms, we will explore several possible failure modes of an image sensor and mechanisms to detect those failures.

Faults that affect individual pixels may appear to have minimal impact to an ADAS system. However, considering the fact that many of the most advanced object detection algorithms can detect objects in the image of less than 10 pixels $\times$ 10 pixels, individual pixel errors, and certainly error clusters, might affect an object identification algorithm. Also, failures that contribute to pixel errors are likely to affect some proportion of pixels across the array. Since a pixel output is

converted to a digital value representing the intensity of light at a given position, a failure can be considered to be any error or corruption that causes any incorrect value, whether static or dynamic. Factors including power delivery, device defects, excessive noise or even ambient radiation could cause errors.

Figure 3. Example of a Fault in the Clock System

Due to the array nature of image sensors, logic associated with the row/column structure of the array may also contribute to device faults. Missing or duplicated rows and/or columns can result in loss of information or incorrect representation of the scene. Obvious errors like a repeating frame in a rear-view system could lead to catastrophic consequences by autonomous, semi-autonomous, and human driving. Even if all elements of the image frame, pixel, row/column and frame data are error-free, transmission errors can cause corruption of the data before it reaches the intended receiver device. These transmission errors can be caused by any number of natural phenomena that themselves are undetectable by the system.

The failures described here are general categories of failures each comprising hundreds of individual failure modes. In fact, there are literally thousands of individual failures in an image sensor that could lead to incorrect data being received by downstream devices. Needless to say that decisions based on the incorrect data could lead to a safety risk. Ultimately, the system must be able to identify and detect the occurrence of these failures in order to take risk mitigating actions.

Challenges in Fault Detection

Detection of faults in an image sensor is a non-trivial exercise. The nature and complexity of the image sensor results in a staggering number of failure modes that could occur. The mix of both analog and digital circuitry further aggravates the problem.

The pixel structure and associated charge transfer and readout circuits are analog in nature. Faults associated with analog circuits have different behavior than those in digital circuits.

During operation, a pixel may suffer from a fault similar to a digital stuck-at fault (which occurs when a logic node becomes “stuck-at” a high or low value). Detecting a fault like a stuck pixel may appear to be trivially done on a host processor. But as sensor resolutions increase to 8 Mpixels and above, checking every pixel for any of several fault conditions on every frame for a given window of time can begin to consume a significant number of processor cycles and memory. Detecting some types of pixel faults, for example noise outside the specified limits, may not even be achievable at the system level. Detecting faults in the analog-to-digital conversion stage, faults that include missing codes, noise, and non-linearities, may also be prohibitive or impossible to perform on a host processor or at the system level.

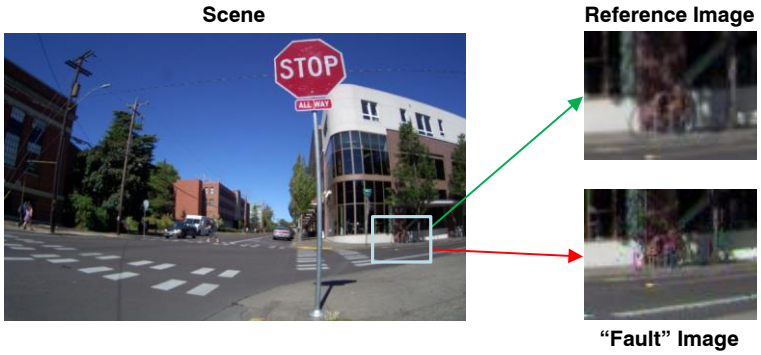

Figure 4. Example of a Fault in the Analog Pipeline

In addition to analog faults at the pixel level, the system must contend with digital faults at the pixel level as well. If pixel data is affected by digital errors that cause bits to be shifted, higher level processing may be unable to even detect these errors. Similarly, while some types of color space errors may be easily visible to the human eye, computing devices may be unable to detect such faults. Systemic faults in the image processing and transmission pipeline can cause widely ranging error behaviors that may or may not be detectable by the system.

Figure 5. Example of a Color Error due to an Image Pipeline Fault

Spatial errors such as row or column addressing errors that result in repeated rows could be detected at the system level but at a cost of CPU cycles and memory. The system has no guarantee that the sensor is even sending the rows and columns in the correct order and virtually no way to verify it. There may be generic methods to determine that consecutive images are similar to prior images, but these may only indicate gross failures in the sensor. More subtle failures are still beyond the scope of the system to detect. Even in cases where detection at the system level is possible, accounting for the vast number of failure modes that are possible and performing the analysis required to detect them would be prohibitive in terms of compute power as well as being incomplete in coverage.

The last three failure modes we could consider are probably more commonly encountered in other digital circuits. The first is ensuring that the data transmitted by the sensor has not been corrupted prior to being received as the data may have to traverse long and noisy transmission media. The second is ensuring that the memories and registers within the sensor are functional and that faults can be detected and/or corrected. The third is a failure in the internal logic or state machines of the sensor.

Figure 6. Example of a Fault in the Row Addressing Logic

The first may be solved by using transmitters and receivers with built in error checking and/or error correcting coding. At the very least this adds cost to the system. The second can be solved by the system by periodically checking the register and memory contents of the sensor, but this consumes system resources. The third could cause issues ranging from catastrophic corruption of image data to more insidious changes that gradually corrupt frame data of the course of many frames. The former type could be easily identified while the latter may be completely invisible to any system level checking.

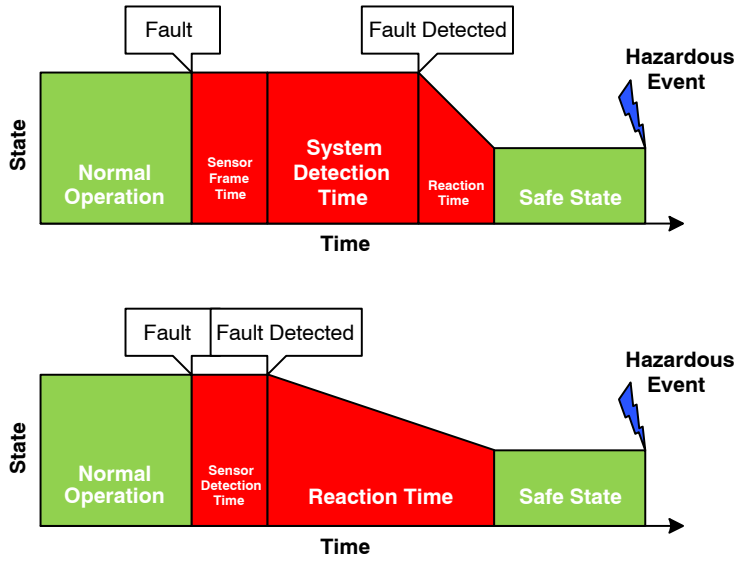

Figure 7. System-based Fault Detection Time vs. Sensor-based Fault Detection Time

Another factor to consider is the delay between the occurrence of the fault, and its detection. Commonly referred to as Fault Detection Time Interval (FDTI), the detection delay has a significant impact on the overall time between the occurrence of the fault and the transition of the system into a safe state before a hazardous event occurs, or Fault Tolerant Time Interval (FTTI), as shown in the illustration above. In the case where the system is required to perform some or all of the fault detection, the overall FDTI includes the time for the sensor to transmit the data to the next stage of the system, as well as the time required for the system to receive, analyze and finally detect the presence of a fault.

In addition to the sheer magnitude of faults to be detected, the potential for undetectable faults at the system level, the additional delay and incremental detection time, the significant compute and memory requirements and the demand to perform these diagnostics in real time, is the hidden cost. The cost to implement fault detection at the system level arises from several contributors. First the additional cost of higher performance CPUs, GPUs and memories, but also the additional development costs incurred to develop the diagnostic algorithms to detect the faults. Increased power consumption and its related thermal dissipation also factor into the cost equation. All of these costs still result in a diagnostic coverage that may have significant weaknesses.

Ultimately, any system level fault detection mechanisms divert resources away from the systems' fundamental goal. This diversion of resources from the systems' primary function adds cost, reduces functionality, or increases complexity impacting the effectiveness, responsiveness, and efficiency of the system. By using sensors with integrated safety mechanisms, system designers can more effectively and efficiently focus resources towards the primary goal.

Advantages of Sensor-based Functional Safety

Sensors today offer a range of test capabilities integrated into the device. Some image sensors provide the ability to transmit a defined test frame. Performing a CRC check on the data could indicate a possible fault in transmission. This is a good first step towards fault detection, but often the test frame does not exercise any significant portion of the actual image capture pipeline, especially the analog portions. This type of check typically only indicates faults in the transmission data path and not in the sensor itself. Additionally, the faults caught by this method tend to be static failures. Finally, the generation of a test frame also takes the sensor, and therefore the entire system, offline for a finite period of time. All of these drawbacks point to the need for a real time method of detecting possible faults at the pixel level of the image sensor.

When considering image sensors for an ADAS or autonomous vehicle system, analog fault coverage should be a serious consideration. More advanced sensors offer significant functional safety mechanisms that provide diagnostics of the analog portion of the sensor, which in most modern sensors occupy more than 50% of the total circuit area. A high level of analog diagnostic coverage is essential to robust image sensor functional safety. A simple metric to differentiate sensors can be the number of analog safety mechanisms supported by the sensor. While certain analog safety mechanisms may require some additional computational, a key factor will be the amount of additional processing required to detect the fault. More advanced safety mechanisms will require less computation, often limited to bounds checking, while less sophisticated mechanisms will require more elaborate, compute intensive processing.

Another step towards safety is the inclusion of a frame counter within the sensor. This allows the system to detect when capture has failed for some reason. Counting pixels and lines can provide even better fault coverage by detecting that the sensor is transmitting the correct number of rows and columns per frame. This may capture dynamic failures, but the detection of missing columns or rows indicates that the fault is fairly severe and renders the frame unusable.

These failure modes produce errors that vary in nature from randomly distributed errors to repetitive or fixed errors that require varying levels of computing power and memory to detect. Individually, detection of a given error could be efficiently performed by any ADAS system processor. While detecting any given type of fault may be possible with some backend processing, detecting every possible type of fault in every frame becomes a monumental task even for the highest performance processors available today. Having on-sensor functional safety mechanisms that perform the bulk of the fault detection could reduce this monumental computing demand to the simple checking of status or health indicator bits or registers that consume virtually no significant system resources.

In addition to significantly reducing computational demands on the system, sensor based diagnostic coverage can also significantly reduce the Fault Detection Time Interval. By signaling the fault in the image stream, the Detection Time can be reduced from T1 + T2, to only T1 as

shown in the drawing below. With sensors typically running at 60 frames per second (fps), a sensor with a detection time of one frame can reduce the FDTI to about 16 ms. This gives the system additional margin and increases the available Fault Reaction Time Interval.

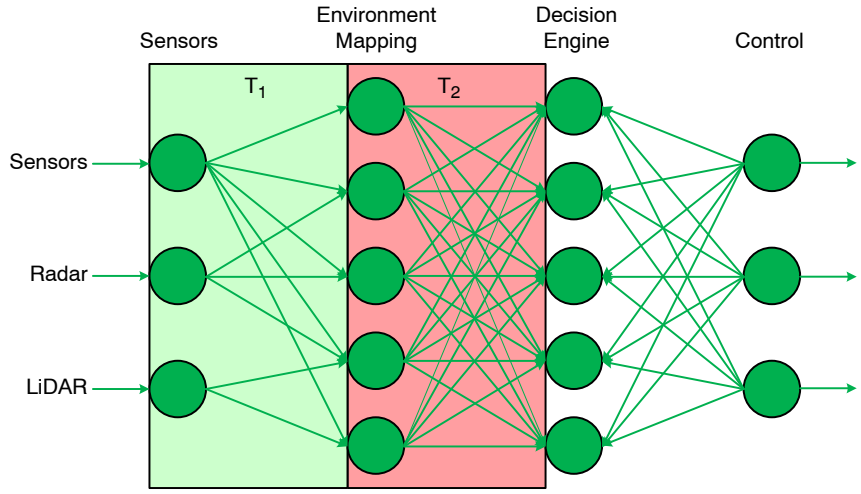

Figure 8. Autonomous Driving System Model with Fault Detection Times

The most advanced functional safety devices today take into consideration the wide range of failure modes that could occur in an image sensor and offer three key advantages. First, the ability to the lowest latency from failure to notification. Second, the ability to provide safety notification in real-time, without affecting the operation, quality, or performance of the sensor. And finally, to offer the highest fault coverage at the lowest computation and cost.

Fault Coverage and Verification

Many image sensor vendors make bold claims of high fault coverage including ASIL−B and ASIL−C support, but how can Tier 1 manufacturers and OEMs verify these claims? Another important factor to consider is the ability to develop a system with higher fault coverage incorporating a sensor with a lower ASIL level, i.e. ASIL decomposition. Here we will examine how diagnostic coverage is typically determined and address the questions of verification and ASIL decomposition.

Typically, diagnostic coverage is based on guidelines given in ISO 26262−5 Annex D. However, the same source is careful to identify that: “The assignment of the faults and their corresponding safety mechanisms to diagnostic coverage levels can vary from that listed in Table D.1”.

However, many sensor manufacturers quote these numbers solely based on the type of test implemented, with little or no consideration of the details of the implementation or any of the other variations presented with the above quoted clause in ISO26262−5 Clause D.1. This usually results in artificially high diagnostic coverage estimates and of course, to the benefit of

the sensor vendor, an equally artificially high ASIL rating. This begs the question of how to accurately determine diagnostic coverage of safety mechanisms.

The best way to determine diagnostic coverage is through actual fault injection to determine if a given fault is detected by a safety mechanism. However, with the number of gates in a typical image sensor being in excess of 1.5 million, exhaustive fault injection is practically infeasible. In addition, automotive image sensors today can contain over 8 million pixels in addition to other analog circuitry. To address this, statistical methods can be employed that enable the calculation of diagnostic coverage within a given margin of error. Statistical fault injection can be effectively used to achieve margins of error of less than 5%. This gives the ability to accurately calculate diagnostic coverage to within a few percent.

When considering the overall safety of an autonomous vehicle, understanding the diagnostic coverage of an image sensor to a high level of accuracy is vital. Having an image sensor whose diagnostic coverage estimation based on recommendations and guidelines creates a high degree of uncertainty when performing the safety analysis of the overall system. Conversely, having an image sensor whose diagnostic coverage is known to be accurate to within a few percent gives high confidence in the overall safety of the autonomous system. Documents such as the FMEDA (Failure Modes, Effects, and Diagnostics Analysis) can give a clear picture of how the safety mechanisms are tested and how diagnostic coverage is calculated.

Conclusion

Clearly, without direct support for detection, protection, and correction of failures within the image sensor itself, the ability for an ADAS system to achieve a desired ASIL levels is severely compromised. Conversely, the ASIL level of the ADAS system can be greatly improved with significant ASIL support directly in the image sensor.

As driving automation increases, the required safety level of the ADAS subsystem will increase. Even today many ADAS systems struggle to meet ASIL−B compliance. In the near term, the number of systems that are required to meet ASIL−B compliance will increase dramatically. Future ADAS systems will be required to meet even more rigorous ASIL−C and ASIL−D compliance. By ASIL decomposition, an ASIL−C ADAS solution could be built only on top of ASIL−B image sensor. In fact, it may even be possible to build an ASIL−D ADAS system using an ASIL−B image sensor through complimentary safety goals. With designs today targeting car models many years in the future, incorporating image sensors with robust ASIL safety features and mechanisms on-sensor greatly improves the ability of the system to meet higher and higher levels of ASIL compliance while reducing system cost and complexity. Finally, using image sensors with highly accurate calculation of diagnostic coverage through statistical fault injection greatly improves confidence in the overall safety of autonomous vehicle systems.

PUBLICATION ORDERING INFORMATION

LITERATURE FULFILLMENT:
Literature Distribution Center for ON Semiconductor
19521 E. 32nd Pkwy, Aurora, Colorado 80011 USA
Phone: 303−675−2175 or 800−344−3860 Toll Free USA/Canada
Fax: 303−675−2176 or 800−344−3867 Toll Free USA/Canada
Email: orderlit@onsemi.com

N. American Technical Support: 800−282−9855 Toll Free USA/Canada
Europe, Middle East and Africa Technical Support:
Phone: 421 33 790 2910

ON Semiconductor Website: **www.onsemi.com**

Order Literature: http://www.onsemi.com/orderlit

For additional information, please contact your local Sales Representative