AIST
Create the Future, Collaborate Together

CPSEC

Overview of security problems for CMOS Image Sensors for Automotive: Opportunity for SESIP?

Kota Ideguchi
Cyber Physical Security Research Institute (CPSEC), AIST

(in collaboration with **Shinji Sato, Hirotaka Yoshida** (CPSEC, AIST))

This presentation is based on results obtained from a project, JPNP23013, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

22/05/2025
GlobalPlatform Cybersecurity Vehicle Forum

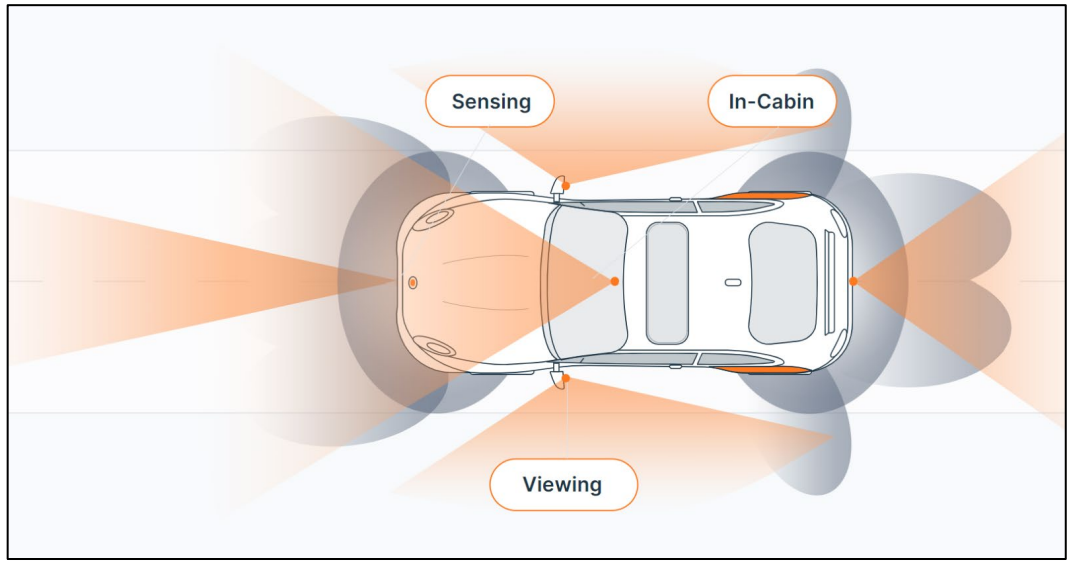
Cyber Physical Security Research Institute (CPSEC), AIST

Our research goal is to promote research on security enhancement technologies, evaluation technologies, and security assurance schemes to realize security in a society where cyber/physical space is highly integrated (**cyber-physical security**), and to contribute to economic development and the realization of solutions to social issues.

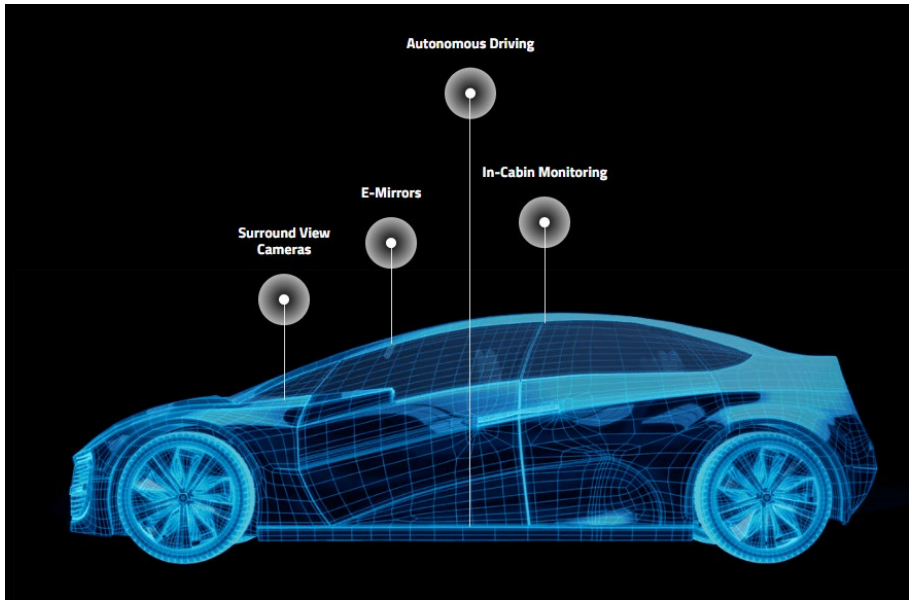
Table of Contents

1-1. Background

In AD/ADAS, CMOS image sensors (CIS) are used for perception of environment and traffic sign detection, lane detection, collision avoidance, parking assistance and so on.



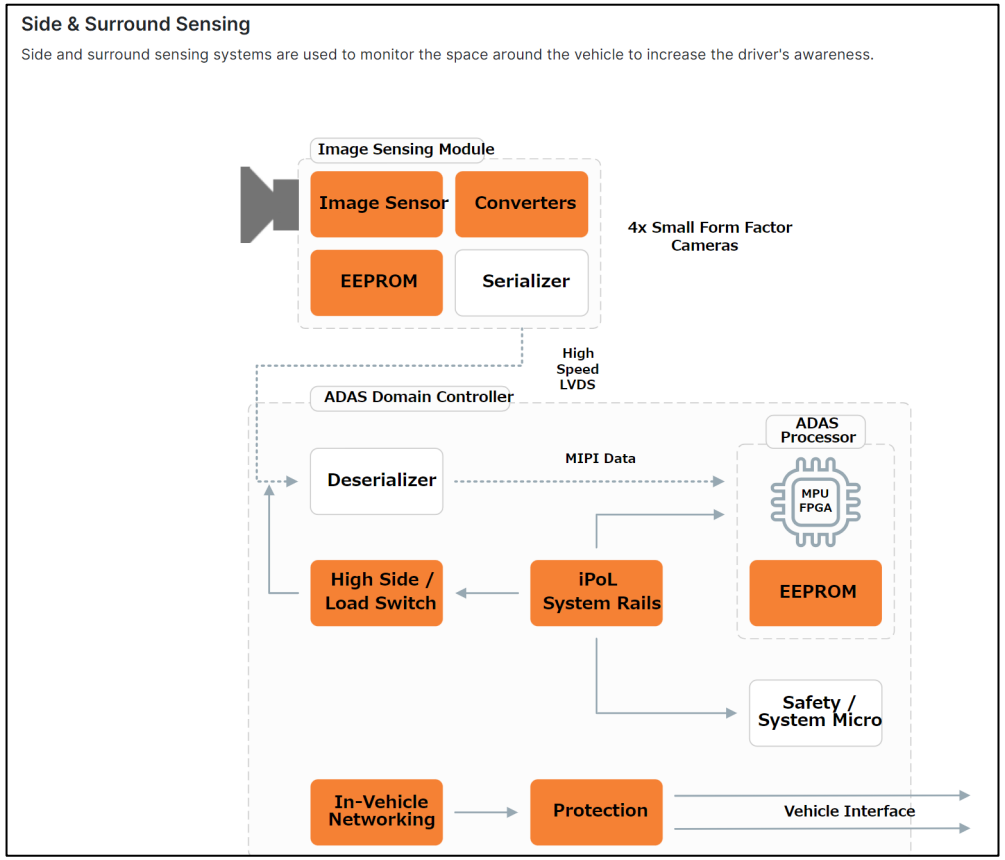
From ON Semiconductor Corporation's webpage
<https://www.onsemi.com/solutions/automotive/adas>



From OMNIVISION's webpage
<https://www.ovt.com/applications/automotive/>

1-2. Background

CISs are connected to ADAS/AD ECUs and send image data to the ECUs, where the data are processed for perception of environment.



From ON Semiconductor Corporation's webpage
<https://www.onsemi.com/solutions/automotive/adas/sensing>

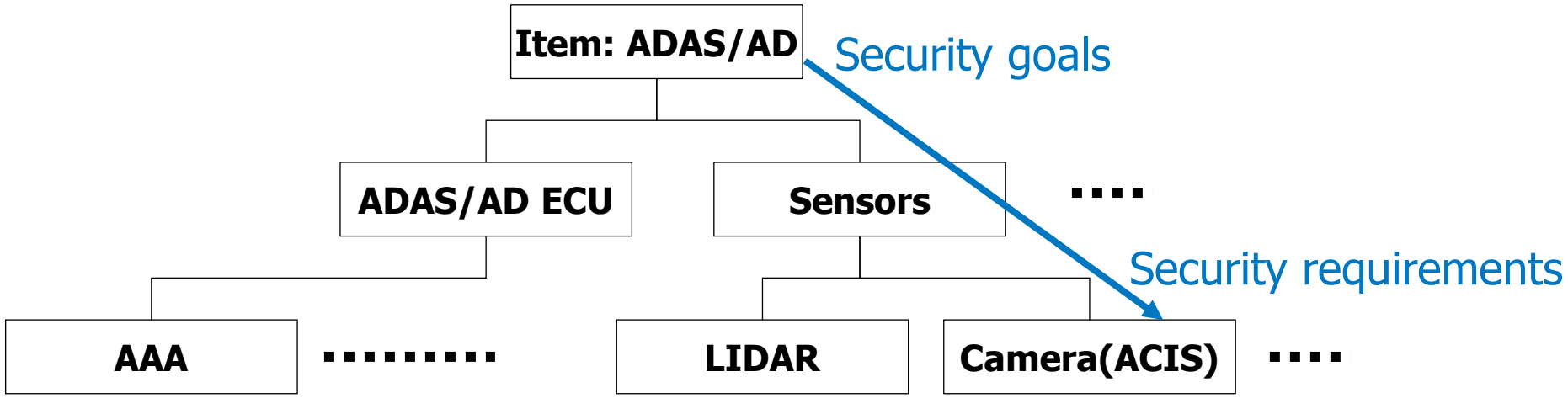
1-3. Background

Cyberattacks against CIS might cause faulty perception which threatens ADAS/AD functionalities.

1-4. Security regulation and standard for vehicles and its components

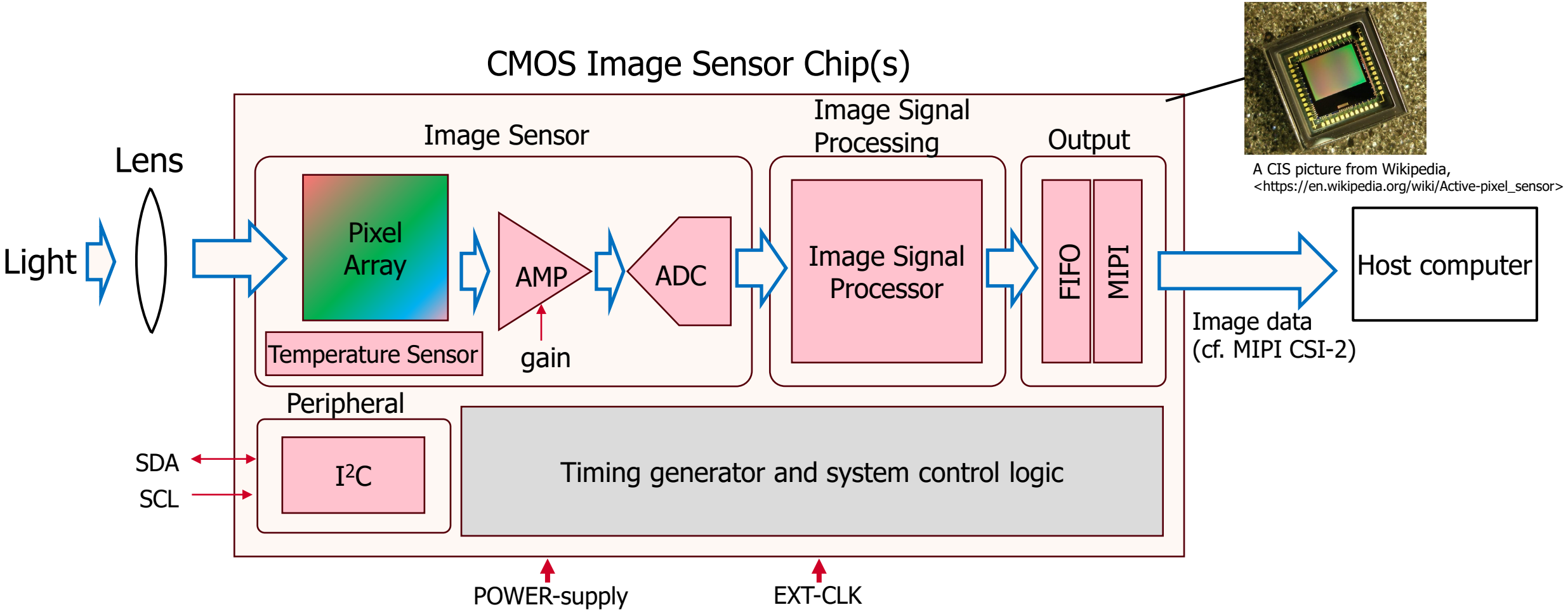
AIST Create the Future, Collaborate Together

- Vehicle cybersecurity is regulated by UNR-155.
- Vehicle cybersecurity is engineered with ISO/SAE 21434.
- Automotive CISs would be influenced with the regulation and standard.



2-1. Overview of a typical Automotive CIS

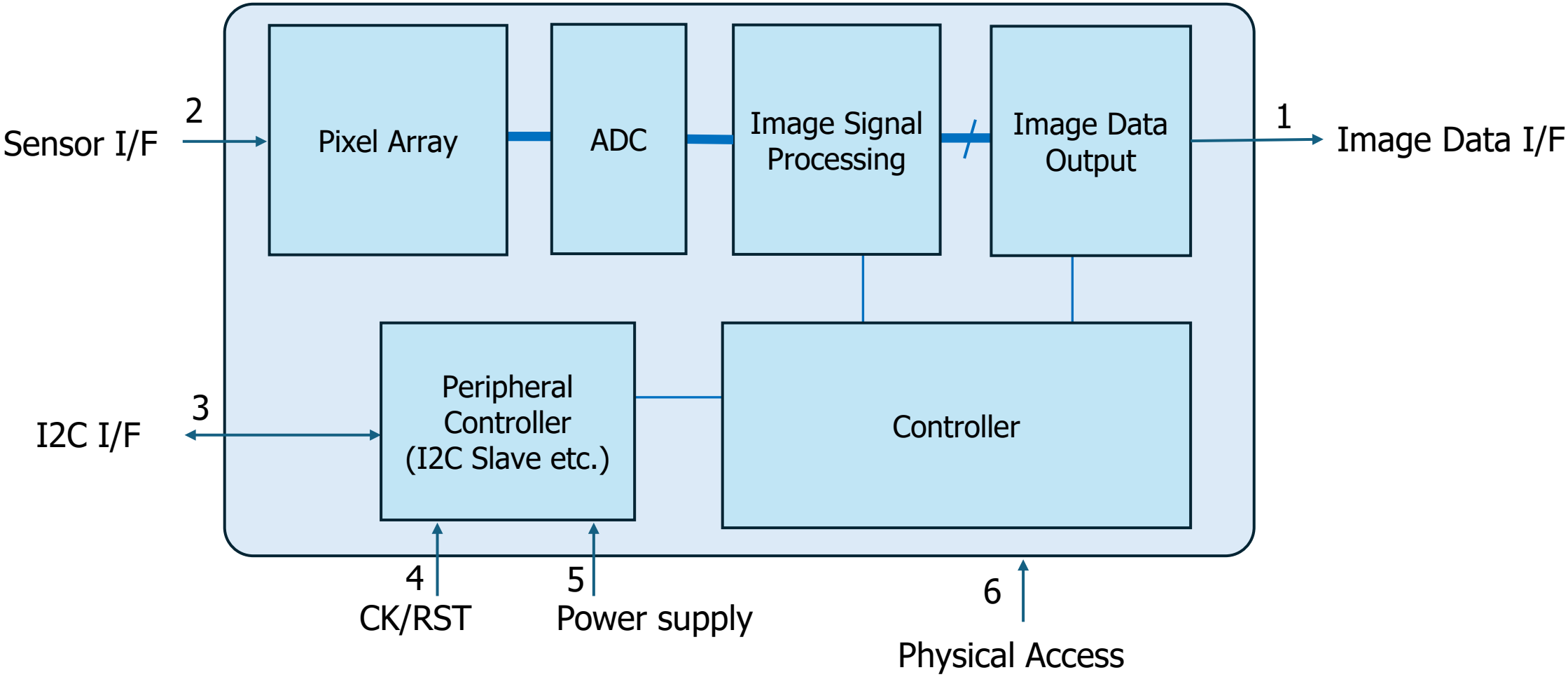
Incoming light from the environment is processed and its image data is sent to a host computer.



A CIS picture from Wikipedia,
<https://en.wikipedia.org/wiki/Active-pixel_sensor>

Abbreviation	AMP(Amplifier)、ADC(Analog to Digital Converter)、FIFO(First-In, First-Out Buffer)、MIPI(Mobile Industry Processor Interface)、CSI-2(Camera Serial Interface 2)、I²C(Inter-Integrated Circuit)、SDA(serial data line)、SCL(serial clock line)

2-2. Example of TOE configuration and attack surface



3-1. Threats for Automotive CIS

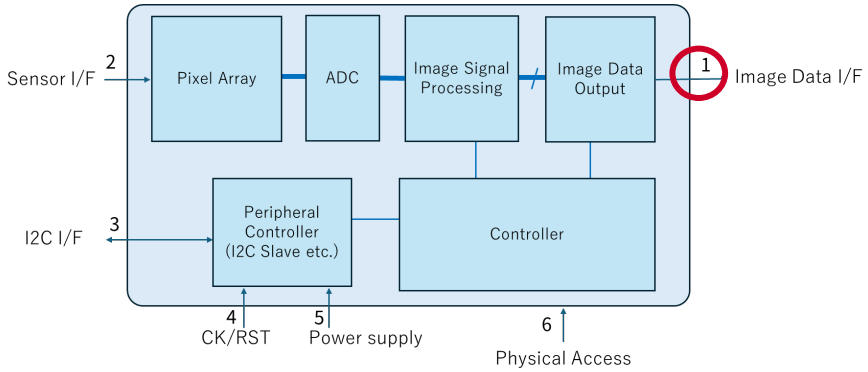
AIST
Create the Future, Collaborate Together

Examples of threats against assets of Automotive CIS

#	Threat	Description	Example references
1	Tampering image data	Image data is maliciously altered, which might result in faulty perception by a host computer.	[1][2]
2	Disclosing image data	Image data with privacy information is leaked to unauthorized entities.	[3]
3	Availability loss of image data	Image data cannot be accessible nor usable, which might degrade perception accuracy of a host computer.	[4]
4	Tampering incoming light	Incoming light from environment is maliciously manipulated, which might cause degradation of image.	[5]
5	Tampering I2C command data	Maliciously altered I2C commands make CIS in abnormal configuration, which might damage sensors or degrade images.	[6]
6	Spoofing CIS itself	Authenticity of CIS is compromised and counterfeit/unauthorized sensor is connected to a host computer.	-
7	Tampering configuration data	Configuration data (exposure, gain, white balance, etc) is maliciously altered, which might cause quality issue of image.	[7]
	⋮	⋮	⋮

3-2. Attack example 1 – Man-in-the-Middle attack on a signal line

#	Threat	Attack surface
1	Tampering image data	Image data I/F



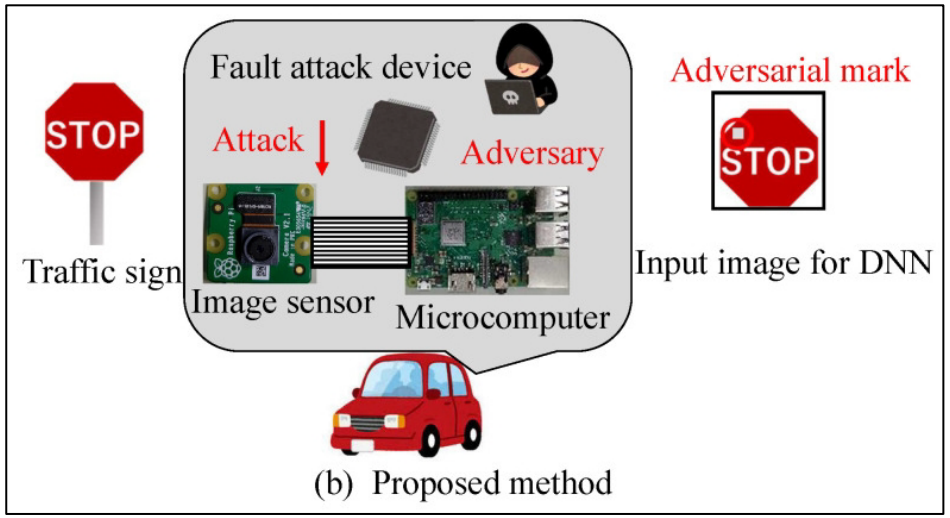


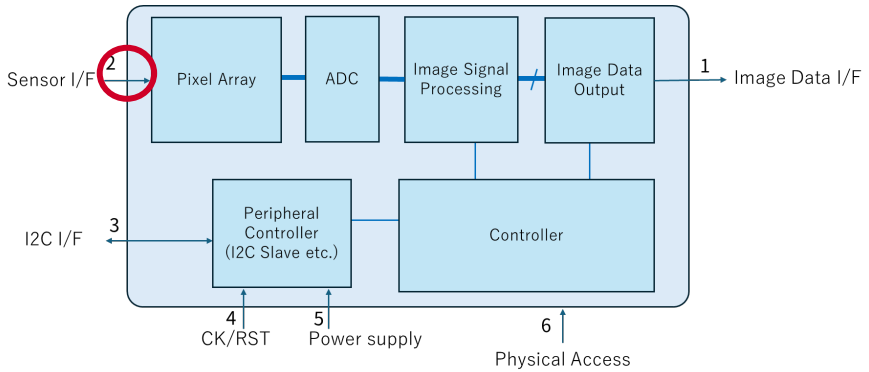
Figure: Attack overview[2]

[2] Oyama *et al.*, "Backdoor Attack on Deep Neural Networks Triggered by Fault Injection Attack on Image Sensor Interface," Sensors, 23(10):4742, 2023,

- Attacker model
  - Physical access to a target vehicle and its internal network cable connected to image data I/F.
- Assumption for CIS
  - Image data sent from CIS don't have integrity check code, such as MAC or signature.
- Attack procedure
  1. An attacker accesses to vehicle and CIS, then installs a device which can inject data on the signal line between the CIS and a host computer.
  2. The device inject image data on the signal line and the image data (MIPI) sent to the host computer is tampered.
  3. Perception of the host computer is affected by tampered image, which might cause faulty perception.

3-3. Attack examples 2 – Blind attack

#	Threat	Attack surface
2	Tampering incoming light	Sensor I/F



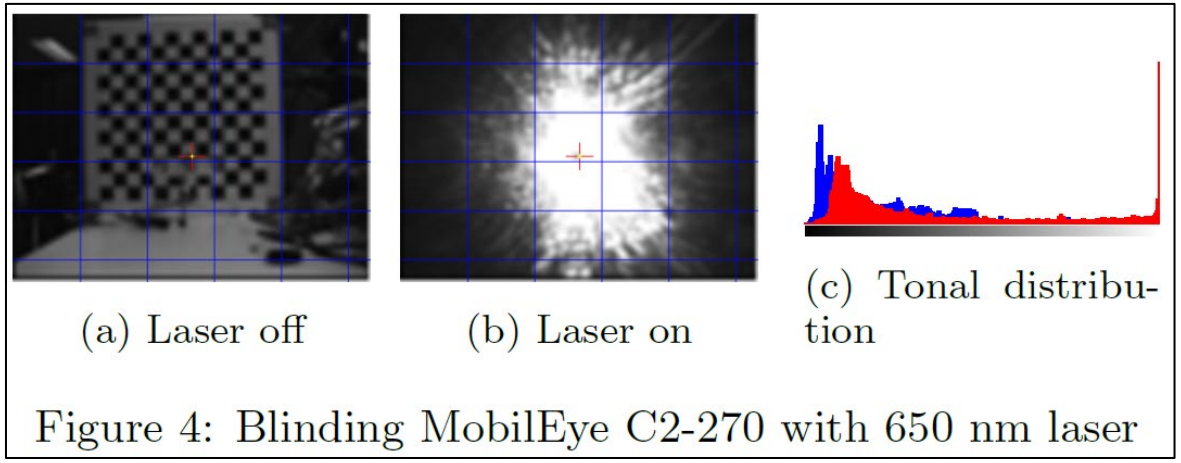


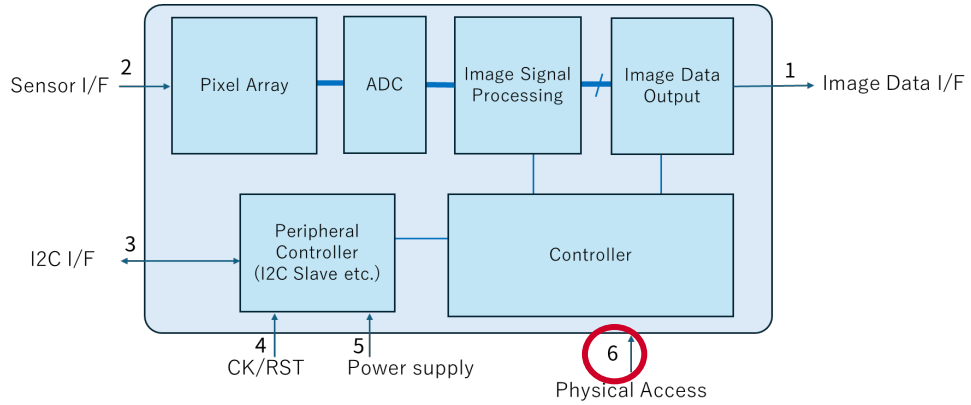
Figure: An Example of blind attack[5]

[5] Petit et al., "Remote Attacks on Automated Vehicles Sensors Experiments on Camera and LiDAR", Blackhat Europe, 2015,

- Attacker model
  - Attacker can emit light to pixel array of CIS from close range.
- Attack procedure
  1. An attacker with a light source approaches the camera module of the target vehicle.
  2. The attacker emits light to pixel array.
  3. CIS cannot control exposure and gain, then the image becomes white out. Objects in environment are hidden from CIS.

3-4. Attack example 3 – replacement to a counterfeit Automotive CIS

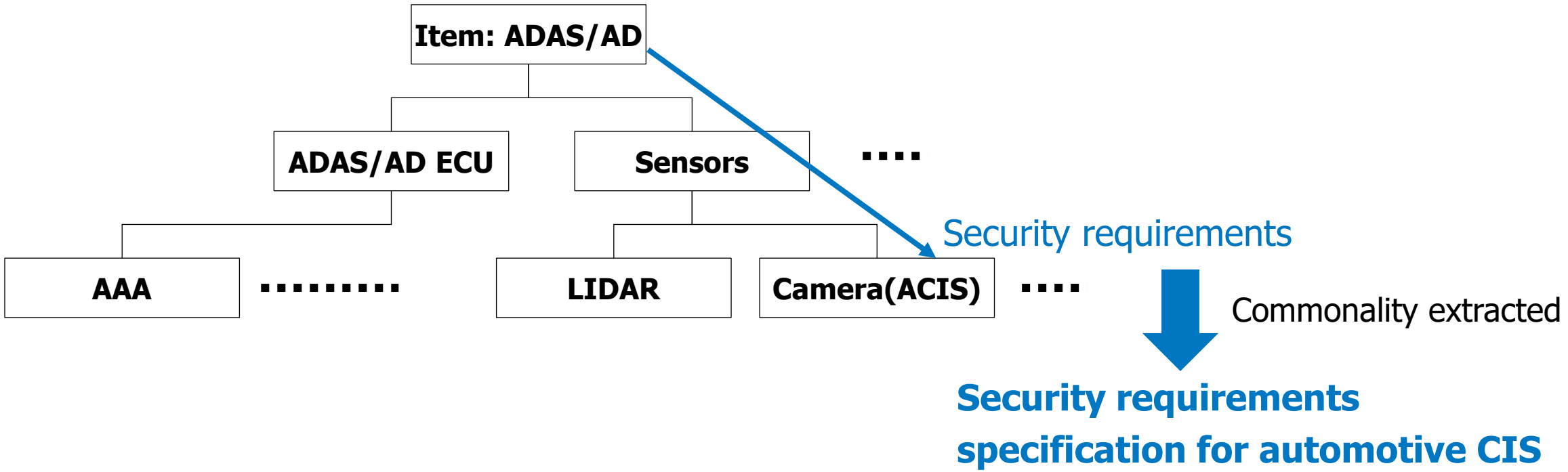
#	Threat	Attack surface
3	Spoofing CIS itself	Physical access



- Attacker model
  - Physical access to a target vehicle and its CIS.
- Assumption for CIS
  - Authenticity of CIS is not checked by a host computer.
- Attack procedure
  1. An attacker accesses to a CIS, then replace it with a counterfeit CIS.
  2. The counterfeit one spoofs an original CIS but has a degraded quality, which causes serious problems of vehicle AD/ADAS functionalities.

4-1. CPSEC Objectives: Security Requirements Specification of Automotive CIS

- CPSEC would like to make a Security Requirements Specification (SRS) for automotive CIS.
- The SRS consists of security requirements common to several vehicle models and camera models, which would be beneficial to automotive industries.



4-2. Assets of the digital part of the Image Sensor

- Data
  - Image data
    - Image data
    - Meta data of image data
  - Incoming light
  - I2C communication data

    I2C command and its reference data: integrity and authenticity shall be protected
  - Configuration data
  - Security parameters
- Functions
  - Functionality of TOE
    - Functionality of sensing incoming light
    - Functionality of signal processing
    - Functionality of transmission of the image data

4-3. Security requirements examples (corresponding SESIP SFRs)

AIST
Create the Future, Collaborate Together

Examples of SFRs to mitigate risks of the attack examples.

Man-in-the-Middle attack on a signal line:

- Secure Communication Support
- Secure Communication Enforcement

Blind attack:

- Availability Support?

Replacement to a counterfeit CIS:

- Verification of Platform Identity
- Attestation of Platform Genuineness

5. Consideration in future

- Which part of Automotive CIS is included in TOE of security requirements specification?
  - Is sensor I/F within the scope?
- Assumptions for attacker, TOE and environment?
  - Physical access allowed?
- Assurance level?

6. Conclusion

- Overview of CMOS Image Sensor for Automotive
- Cybersecurity threats for Automotive CIS
- Security Requirements Specification for Automotive CIS

References

[1] Oyama *et al.*, "Fundamental Study of Adversarial Examples Created by Fault Injection Attack on Image Sensor Interface," AsianHOST'22, 2022,
[2] Oyama et al., "Backdoor Attack on Deep Neural Networks Triggered by Fault Injection Attack on Image Sensor Interface," Sensors, 23(10):4742, 2023,
[5] Petit et al., "Remote Attacks on Automated Vehicles Sensors Experiments on Camera and LiDAR", Blackhat Europe, 2015,
[6] Gomez-Bravo et al., "Hardware Attacks on Mobile Robots: I2C Clock Attacking," Robot 2015,
[7] Khelif et al., "Non-invasive I2C Hardware Trojan Attack Vector," 2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp.1-6, 2021.