

SESIP Automotive Profile: Automotive CMOS Image Sensor Profile

Kota Ideguchi, Shinji Sato, Hirotaka Yoshida
CPSEC, AIIST
2025.12.09

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



Cyber Physical Security Research Institute (CPSEC), AIST

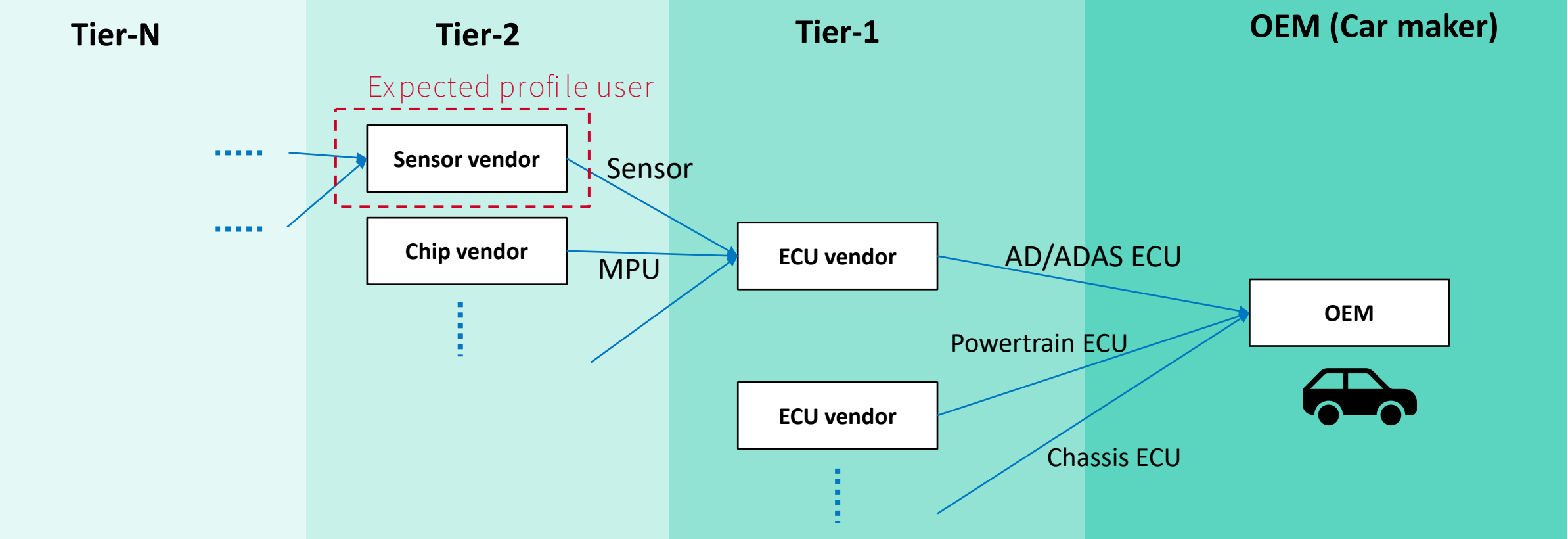
Our research goal is to promote research on security enhancement technologies, evaluation technologies, and security assurance schemes to realize security in a society where cyber/physical space is highly integrated (**cyber-physical security**), and to contribute to economic development and the realization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

1. ACIS overview
 1. How to determine TOE
2. Security Requirements
3. Attack Examples
4. SESIP levels

1. ACIS overview

Vehicles are developed and manufactured with huge number of companies consisting supply-chain.

A typical example of automotive supply-chain related to E/E architecture:



The connected vehicle device (CVD) is defined as a combination of ECU and its sensors/actuators. This document covers specific types of CVD with Automotive CMOS Image Sensor (ACIS), which is depicted in Figure 3 1.

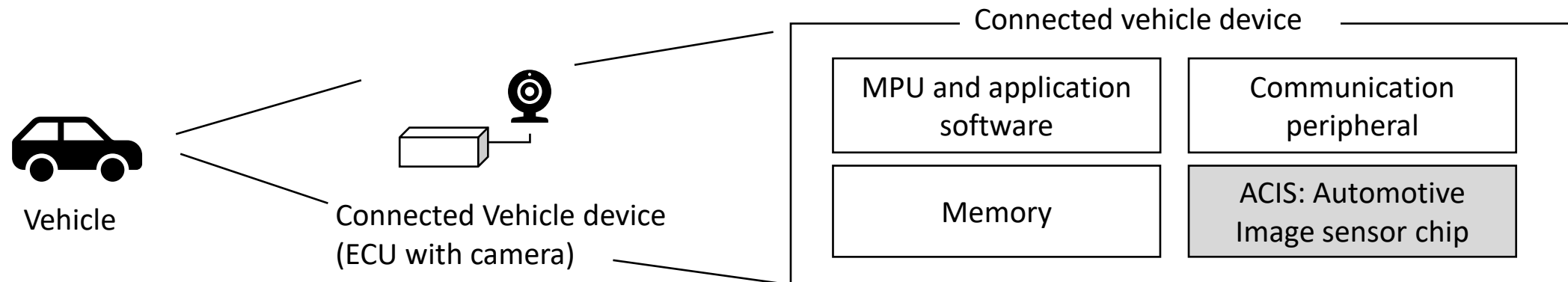


Figure 3-1 ACIS for connected vehicle device and environment

The platform is a single-chip product integrating pixel array, image signal processor, input/output circuits and control circuits.

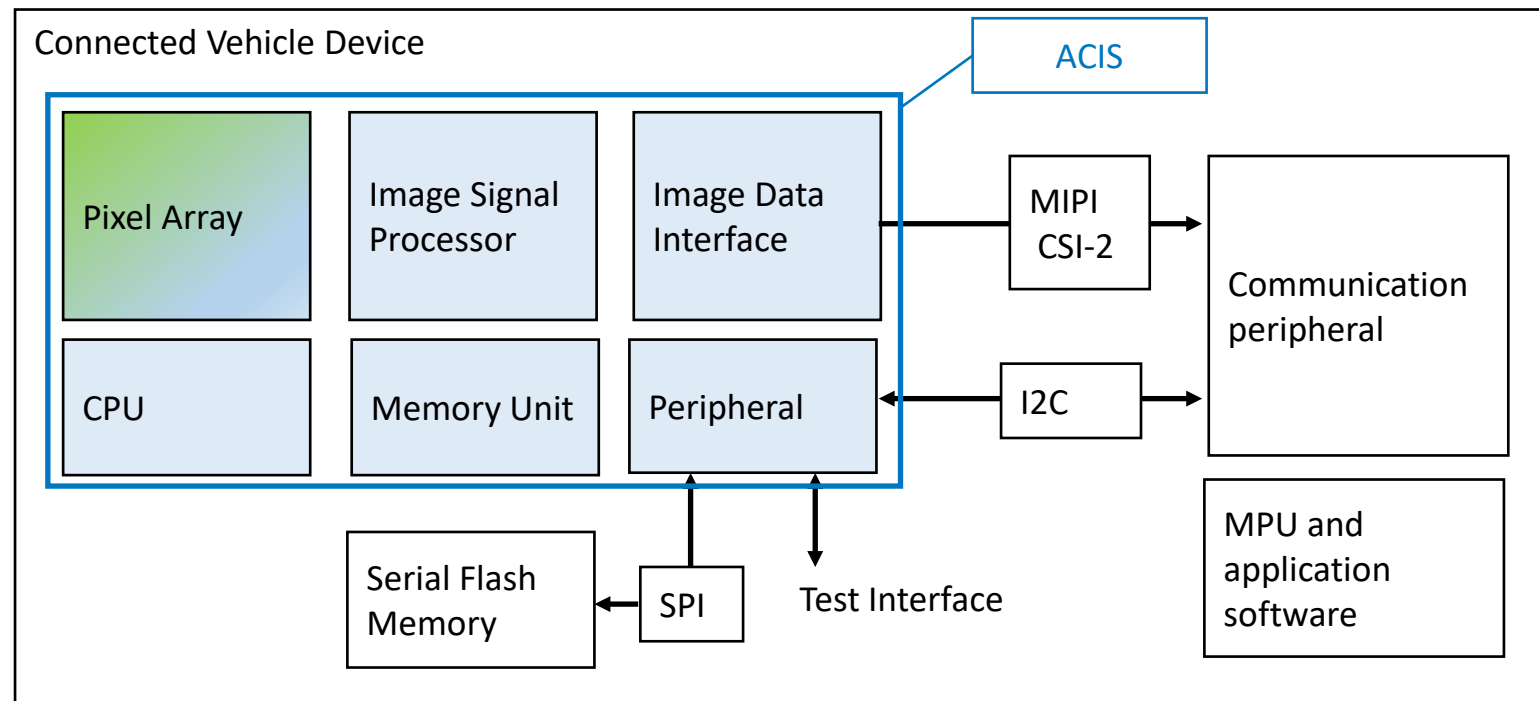
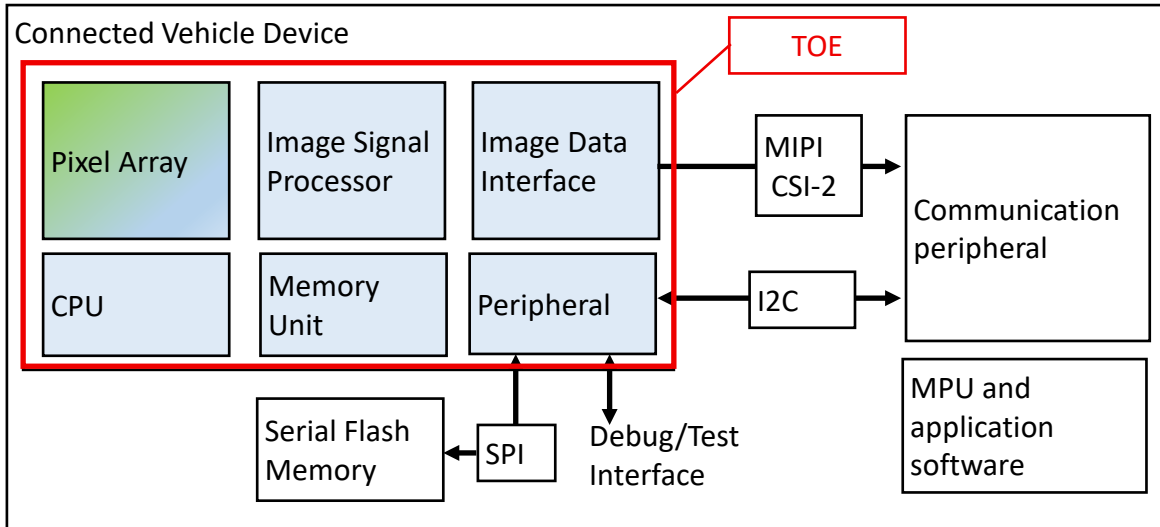


Figure 3-2 Components of ACIS

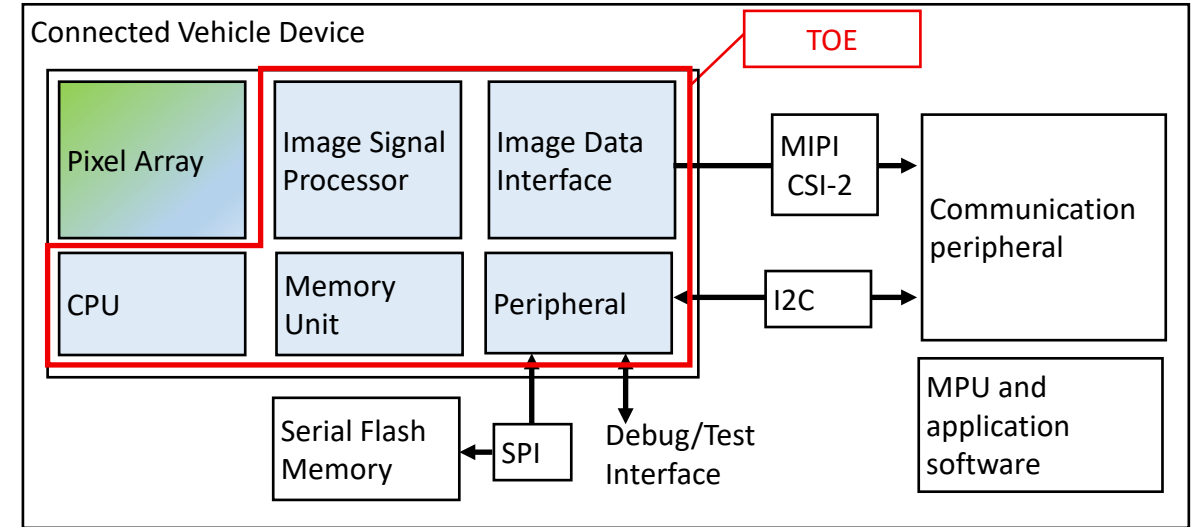
- Cyberattacks against pixel array is out of scope.
- An ACIS is connected to a host computer (MPU of CVD) and communication of image data and command data between the ACIS and the host is an intrinsic function of ACIS.

Several TOE candidates are considered and compared.

- Model A: A whole of ACIS

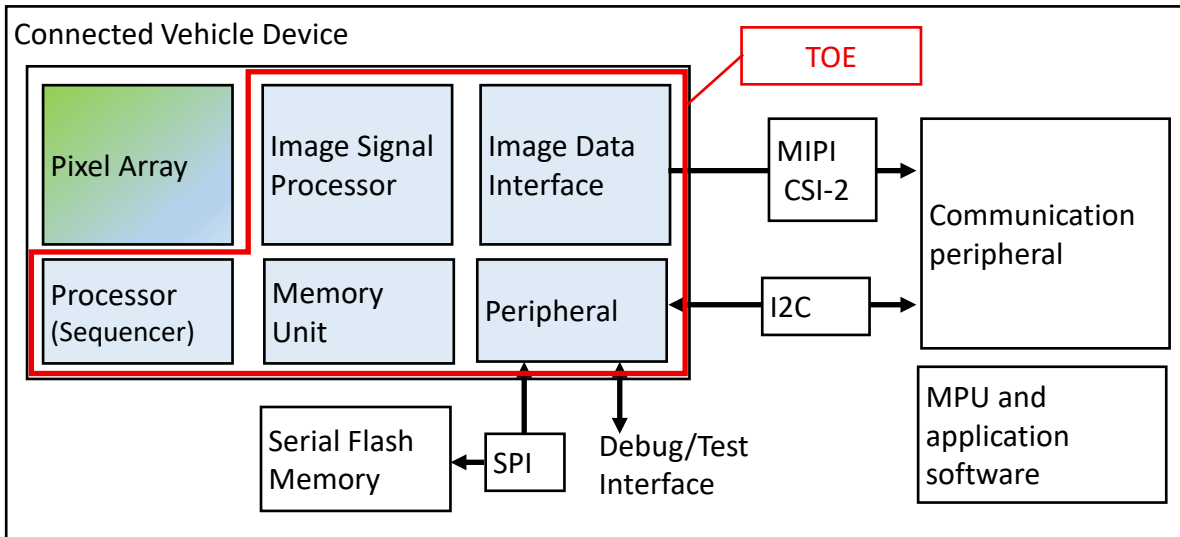


- Model B: ACIS excluding Pixel Array

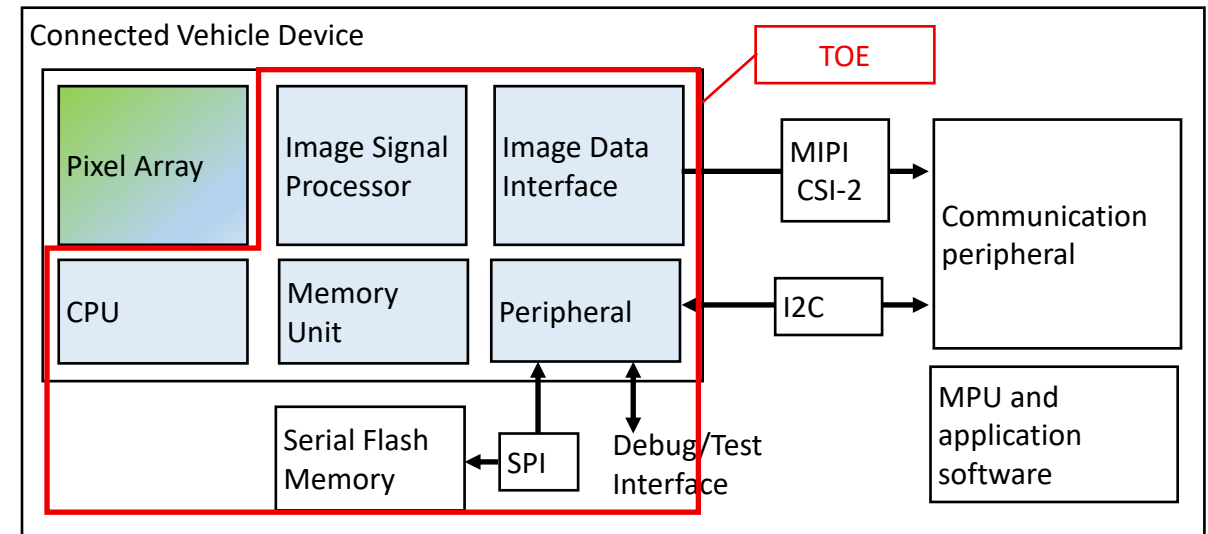


Several TOE candidates are considered and compared.

- Model C: Model B with sequencer instead of CPU

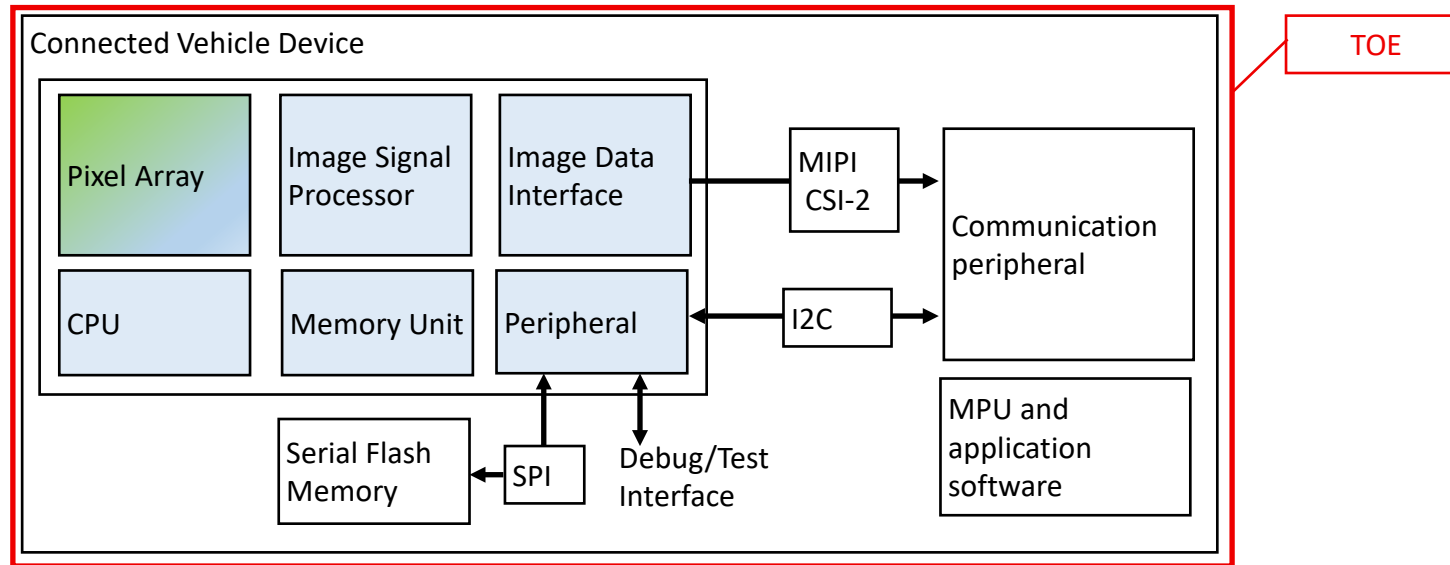


- Model D: Model B and external memory



Several TOE candidates are considered and compared.

- Model E: A whole of CVD



TOE

Model B is a given condition of an ACIS vendor we are discussing with.

Compared with the other models, we consider the Model B is relevant to become a TOE for ACIS profile.

TOE	Short description	Pros	Cons
Model A	A whole of ACIS	<ul style="list-style-type: none"> Boundary is simple. 	<ul style="list-style-type: none"> Difficulties and complexities to prevent physical attacks against pixel arrays.
Model B	ACIS excluding Pixel Array	<ul style="list-style-type: none"> Condition given from an ACIS vendor. 	
Model C	Model B with sequencer instead of CPU	<ul style="list-style-type: none"> Broader range of ACIS can become targets. 	<ul style="list-style-type: none"> The MCU/MPU profile cannot be used as base.
Model D	Model B and external memory	<ul style="list-style-type: none"> Stored configuration data can become protected assets, which makes logical scope more self-contained. 	<ul style="list-style-type: none"> In case of a poor CPU performance of ACIS, security of data on external memory might be addressed by ECU not ACIS.
Model E	A whole of CVD	<ul style="list-style-type: none"> Boundary is simple. 	<ul style="list-style-type: none"> Responsibility for security of CVD is taken by ECU vendors, not ACIS vendors.

2. Security Requirements

The typical core security features of the TOE are:

- Verification of platform identity and platform instance identity, to verify correctness of the TOE
- Secure communication support and enforcement, to protect communication between the platform and the CVD
- Secure initialization, to control the platform's initialization sequence

Optional packages may be selected depending on the context of use of the platform:

- Attestation of the platform identity and platform instance identity, to verify TOE's genuineness
- Secure update for life cycle handling
- Secure debugging in case of investigation need
- Secure data serialization, to protect the integrity of data for ACIS
- Cryptographic operations, often based on hardware cryptographic accelerators
- Hardware protections to handle hostile environments

There are differences in mandatory requirements between the MCU/MPU profile and ACIS profile.

#	SEVIP SFR	MCU/MPU profile	ACIS profile	Reason of difference
1	Verification of Platform Identity	Base SP	Mandatory	
2	Secure Initialization of Platform	Base SP	Mandatory	
3	Secure Update of Platform	Base SP	Optional	ACIS might not have SW.
4	Secure Debugging	Base SP	Optional	ACIS might not have a debug port.
5	Residual information purging	Base SP	Not adopted	ACIS might have only one process.
6	Verification of Platform Instance Identity	-	Mandatory	A counterfeit of ACIS must be precluded.
7	Secure Communication Support	-	Mandatory	Communication with the host is intrinsic for ACIS.
8	Secure Communication Enforcement	-	Mandatory	

5.2.1 Verification of Platform Identity

The platform provides a unique identification and version of the platform.

The CVD must be able to query:

- The version of the platform firmware
- The identification and the version of the platform hardware

5.2.2 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform.

The CVD must be able to query the identification of individual platform hardware.

5.2.3 Secure Initialization of Platform

The platform ensures its authenticity and integrity and data used for correct operation during platform initialization. If platform authenticity or integrity cannot be ensured, the platform will go to <list of controlled states>.

5.2.4 Secure Communication Support

The platform provides one or more secure communication channel(s).

The secure communication channel authenticates the CVD and the platform and protects against disclosure, modification, replay, and impersonation of data between the endpoints, using <list of protocols and measures>.

The protocols and measures must ensure that data requested with confidentiality protection is protected against disclosure, and that data requested with authenticity and integrity protection is protected against modification, replay, and impersonation in such a way that the platform instance cannot be impersonated, thus allowing for secure binding and anti-cloning properties.

Compromising the confidentiality of the keys used in the platform for these protocols and measures constitutes a break of this SFR.

At SESIP3 level, the platform must implement a protocol that provides access to the platform only when authentication performed by the CVD is successful.

5.2.5 Secure Communication Enforcement

The platform ensures that communication with the platform can only be done over the secure communication channel(s) supported by the platform using the protocols described in the SFR “Secure Communication Support” for data requested to be protected for confidentiality, integrity, or authenticity.

5.3.1 Attestation of Platform Genuineness

The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity”, in a way that cannot be cloned or changed without detection.

The ST writer describe here how the ACIS fulfils the requirement and the associated refinements if any.

5.3.2 Secure Debugging

The platform only provides <list of endpoints> authenticated as specified in <specification> with debug functionality.

All assets accessible through the Secure Debugging mechanism shall be protected against unauthorized access.

For debug functionality authentication, device specific credentials shall be used.

The ST writer describes here how the platform fulfils the requirement and the associated refinements if any.

5.3.3 Secure Data Serialization

The platform ensures that all data stored outside the direct control of the platform, except for <list of data stored outside the direct control of the platform>, is protected such that the <selection: confidentiality, integrity, authenticity, binding to the platform instance, versioning> is ensured.

The ST writer describes here how the ACIS fulfils the requirement and the associated refinements if any.

5.3.4 Secure Trusted Storage

The platform ensures that all user data stored, except for <list of data stored in plaintext>, is protected to ensure its integrity, authenticity, and binding to the platform instance.

The ST writer describes here how the ACIS fulfils the requirement and the associated refinements if any.

The mechanism used shall protect both the integrity and authenticity of stored data.

5.3.5 Secure Confidential Storage

The platform ensures that all data stored by the application, except for <list of data stored>, is protected to ensure its confidentiality, integrity, authenticity, and binding to the platform instance.

The ST writer describes here how the ACIS fulfils the requirement and the associated refinements if any.

This SFR can be used for situations where the storage is protected by non-encryption means.

5.3.6 Secure Encrypted Storage

The platform ensures that all user data stored, except for <list of data stored in plaintext>, is encrypted as specified in <specification> with a platform instance unique key of key length <key length>.

The ST writer describes here how the ACIS fulfils the requirement and the associated refinements if any.

5.3.7 Cryptographic Functionality

The platform provides <Operations, see table below> functionality with <Algorithm, see table below> as specified in <Specification, see table below> for key lengths <Key lengths, see table below> and modes <Modes, see table below>.

Table 5-1 Cryptographic operation

The ST writer describes here how the image sensor chip fulfils the requirement and the associated refinements if any.

Informative

This package defines the security requirements needed to cover the use case where the platform is updatable and thus requires protection against illegal updates or patches. These Security Functional Requirements must be claimed in case of configuration **[any code]** (see section 3.3, Use Case).

5.4.1 Secure Update of Platform

The platform can be updated to a newer version in the field such that the confidentiality, integrity, and authenticity of the platform is maintained.

The ST writer describe here how the ACIS fulfils the requirement and the associated refinements if any.

Informative

This package defines the security requirements needed to cover the use case where the platform is physically accessible and thus requires protection against local attacks. These Security Functional Requirements must be claimed in case of configuration **[any user]** (see section 3.3, Use Case).

5.5.1 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

3. Attack Examples

- We wrote some attack examples which will be mitigated by countermeasures satisfying SFRs of ACIS.

#	Attack	Related SFR/Package
1	Replacing an ACIS with a fake one	Verification of Platform Identity Verification of Platform Instance Identity
2	Tampering CMOS image via man-in-the-middle	Secure Communication Support Secure Communication Enforcement
3	Modifying the boot image	Secure Initialization
4	Side-channel analysis to retrieve AES key	Hardware Protections

- Replacing an ACIS with a fake one
 - If the ACIS doesn't have ID verification functionality, an attacker may replace the genuine ACIS with the fake ACIS.

Factor	Description	Ident'n	Exploit'n
Elapsed time	An attacker reads out platform ID and instance ID then writes those IDs to the fake ACIS. He replaces a genuine ACIS with the fake ACIS on the CVD.	≤ one day (1)	≤ one day (3)
Expertise	A layman can read out and write the IDs. A proficient can replace the ACISs due to BGA.	proficient (2)	proficient (2)
Knowledge of TOE	Restricted knowledge for identification. No knowledge require for exploitation.	Restricted (2)	Public (0)
Access to TOE	Only few sample	< 10 (0)	< 10 (0)
Equipment	Standard equipment only	Standard (1)	Standard(2)
Open samples	No	NA	NA
	Sub total	6	7
	Total	13	

SESIP Level 1/2 required

4. SESIP Levels

The claims of the Base SP apply when the ACIS is operating in a non-hostile environment and executing only trusted software (i.e. use cases **[trusted user only]** and **[trusted code only]**).

Packages may need to be added to cover specific features and/or environments, as follows:

- If the product operates in a hostile environment, use case **[any user]**, Package ‘Hardware Protections’ must be added to the claim.

Features claim	Minimum to maximum allowed SESIP levels
Base SP (mandatory) <ul style="list-style-type: none"> • Verification of platform identity • Verification of Platform Instance Identity • Secure initialization of platform • Secure Communication Support • Secure Communication Enforcement Additional SFRs <ul style="list-style-type: none"> • Attestation of platform genuineness • Secure debugging • Secure Data Serialization • Secure Trusted Storage • Secure Confidential Storage • Secure Encrypted Storage • Cryptographic functionality 	SESIP 1 SESIP 2
Base SP + Package ‘Secure Update’ (optional) [any code] (replaces [trusted code only]) Additional SFR: <ul style="list-style-type: none"> • Secure Update of Platform 	SESIP 2
Base SP + Package ‘Hardware Protections’ (optional) [any user] (replaces [trusted user only]) Additional SFR: <ul style="list-style-type: none"> • Physical Attacker Resistance 	SESIP 3

A current draft of SESIP profile for ACIS is explained.

- Expected primary users of the ACIS profile are sensor vendors which are typically Tier-2 suppliers in automotive supply-chain.
- Several candidates of TOE are compared and ACIS with Pixel Array excluded is adopted as our TOE.
- SFRs of the ACIS profile and mapping with the MCU/MPU profile are explained.
- Attack examples are explained and ratings of those were estimated.
- Consideration of mapping to SESIP levels is explained.