The Session on Cyber Security

How to Support Mastering Intrusion Detection System

Tsutomu Matsumoto

tsutomu@ynu.ac.jp

Faculty of Environment and Information Sciences

and

Institute of Advanced Sciences

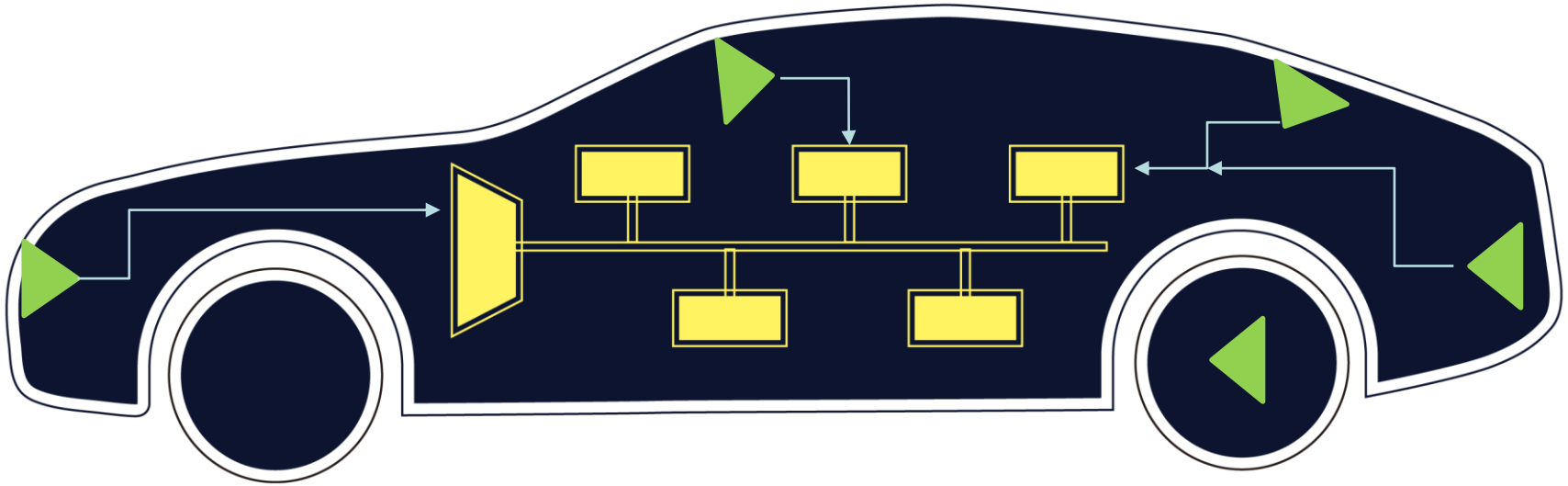
YNU YOKOHAMA National University

IAS Institute of Advanced Sciences Yokohama National University

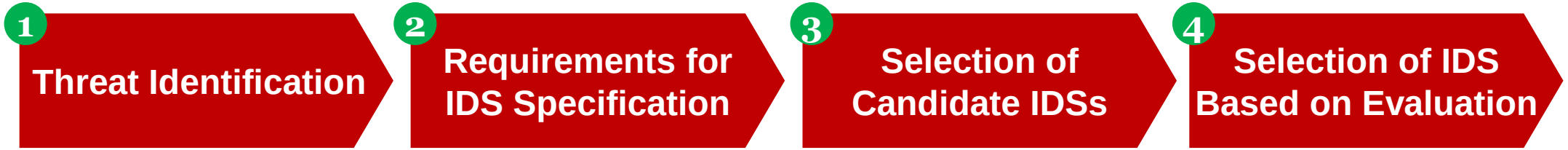
Automotive IDS is useful but difficult-to-use security technology.

In-Vehicle Network

- Cryptography
  - Message Authentication Codes
  - Digital Signatures
  - Encryption
- Cryptographic Key Management
- Anomaly Detection
  - Intrusion Detection System
    - ✓ Host Based/ Network Based
- Security Supply Chain Management

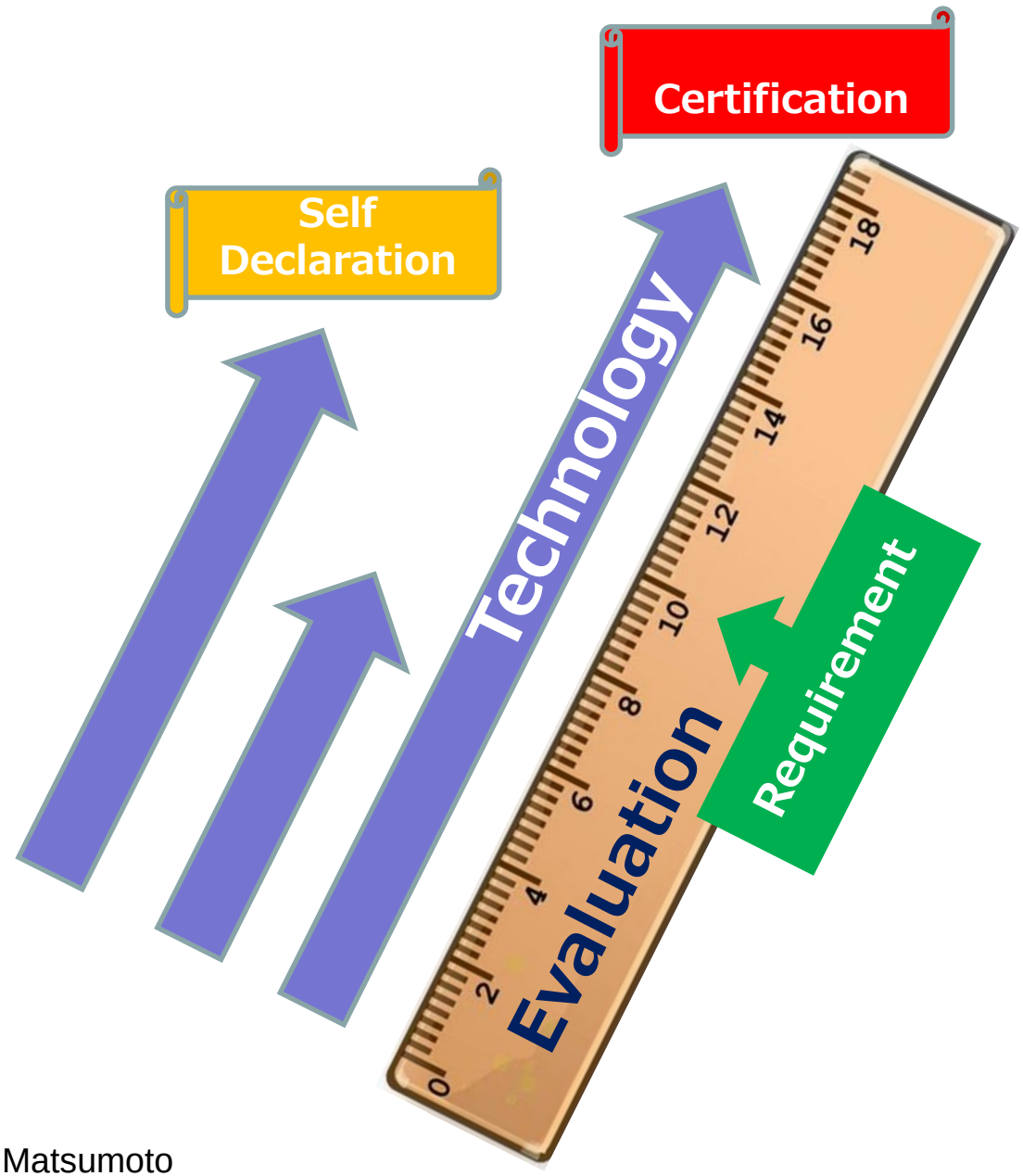


Needs of Guideline for Introducing Automotive IDS



- One of the SIP-adus projects has started to create such a Guideline by collaborating with vehicle industry organizations like Jaspar and OEMs and Suppliers.

Tools Needed for Evaluating and Adopting IDSs



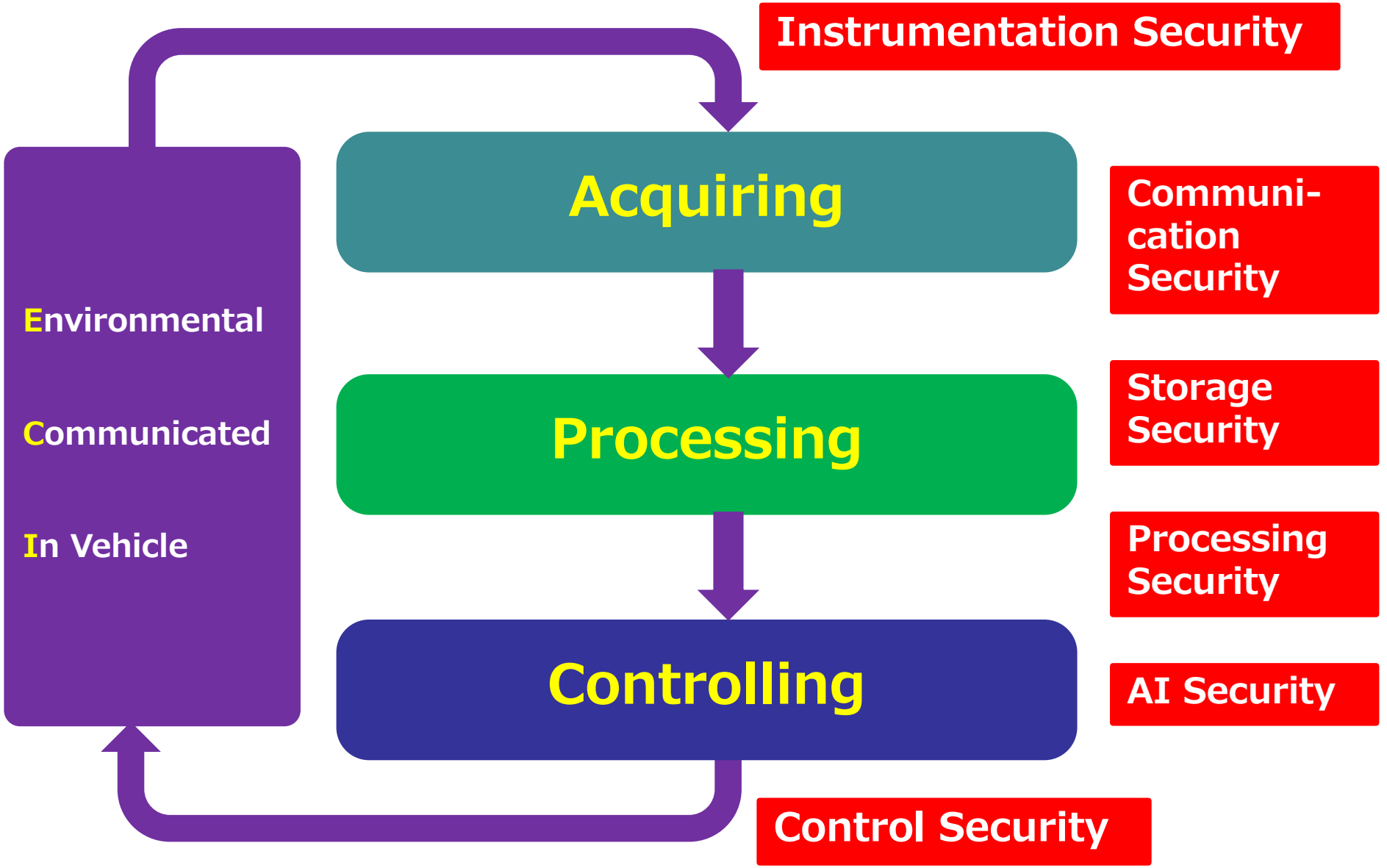
Needs for Developing

1. Evaluation Technologies
2. Security Enhancement Technologies
3. Security Assurance Schemes
   - Self Declaration
   - Certification

How to Describe IDS Specification (provisional)

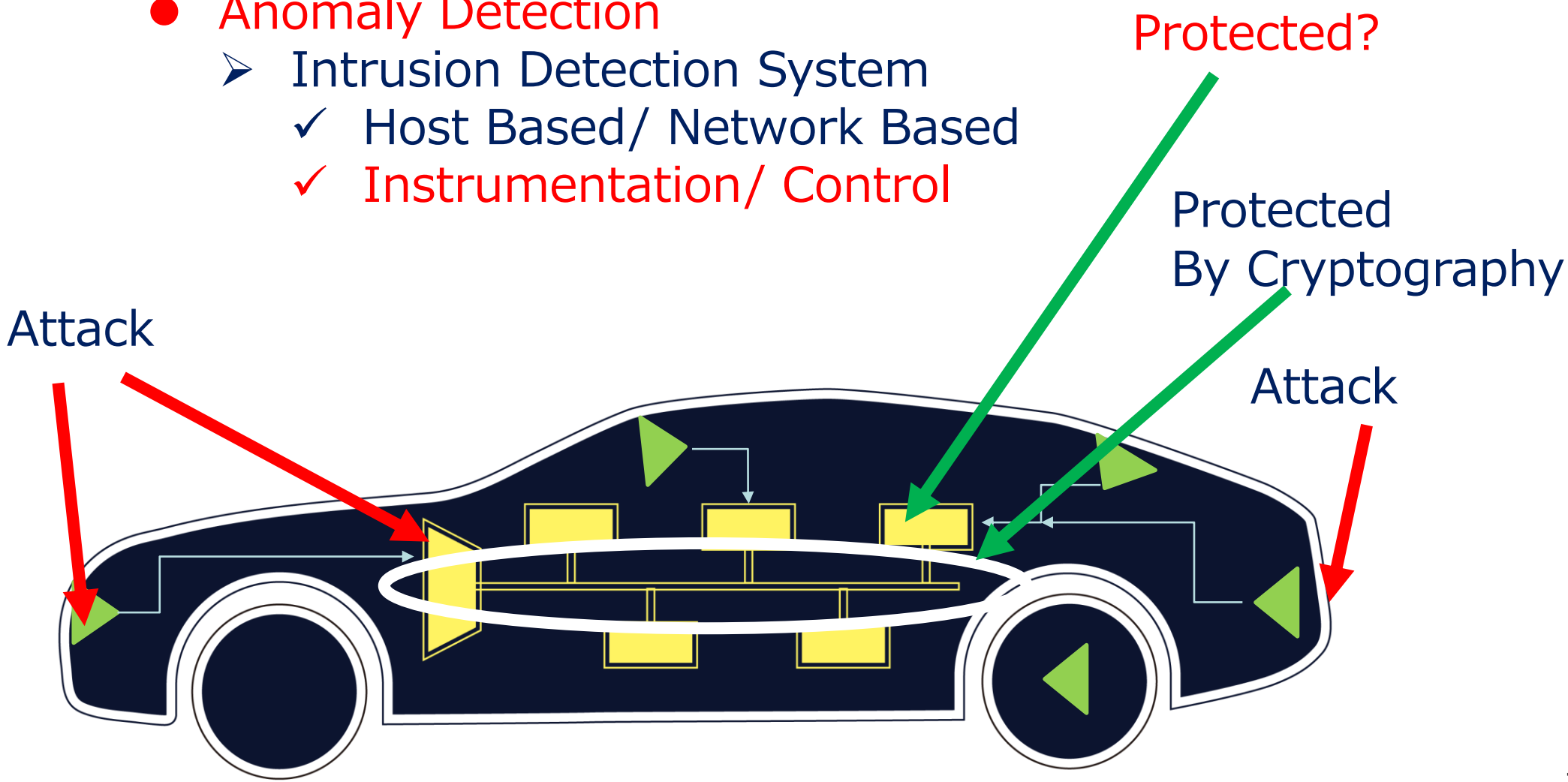
Purpose	Phase	Functionality	Evaluation Items	Type of Quality
Basic Matters			Type of IDS（Network-based IDS/Host-based IDS）	N/A
			Supporting In-vehicle Network Protocols (CAN/CAN-FD/Ethernet/FlexRay/LIN)	N/A
			Methods of Detection (Specification/Anomaly/Signature)	N/A
Detection	Introduction	Calibration	Necessity of DBC File	Usability
			Necessity of Driving Data	Usability
			Diversion Availabiruty of Calibration Information of Existing Models	Portability
	Operation	Detection of Security Events	Accuracy of Detection	Functional Conformity
			Existence and Granurality of Explanation of Detected Security Events	Usability
Response	Introduction	Setting for Notification	Notification Conditions that can be Specified by OEM at the time of introduction	Usability
	Operation	Notification of Seucurity Events	Contents of Notification on Normal and Detected Phases	Functional Conformity
			Where to Notify Security Events	Usability
		Logging of Security Events	Log Contents (Detected Code /Message Contents / State of the Vehicle /Risk, etc.)	Functional Conformity
Recovering	Operation	Update	Method of Updating Program (Via Physical Port/ OTA/ others)	Maintainability
			Method of Updating Signatures and Settings (Via Physical Port/ OTA/ others)	Maintainability
			Role Sharing among the Server for Update, Update Management Module, and IDS	Maintainability

Major Automotive Cyber Physical Security Issues



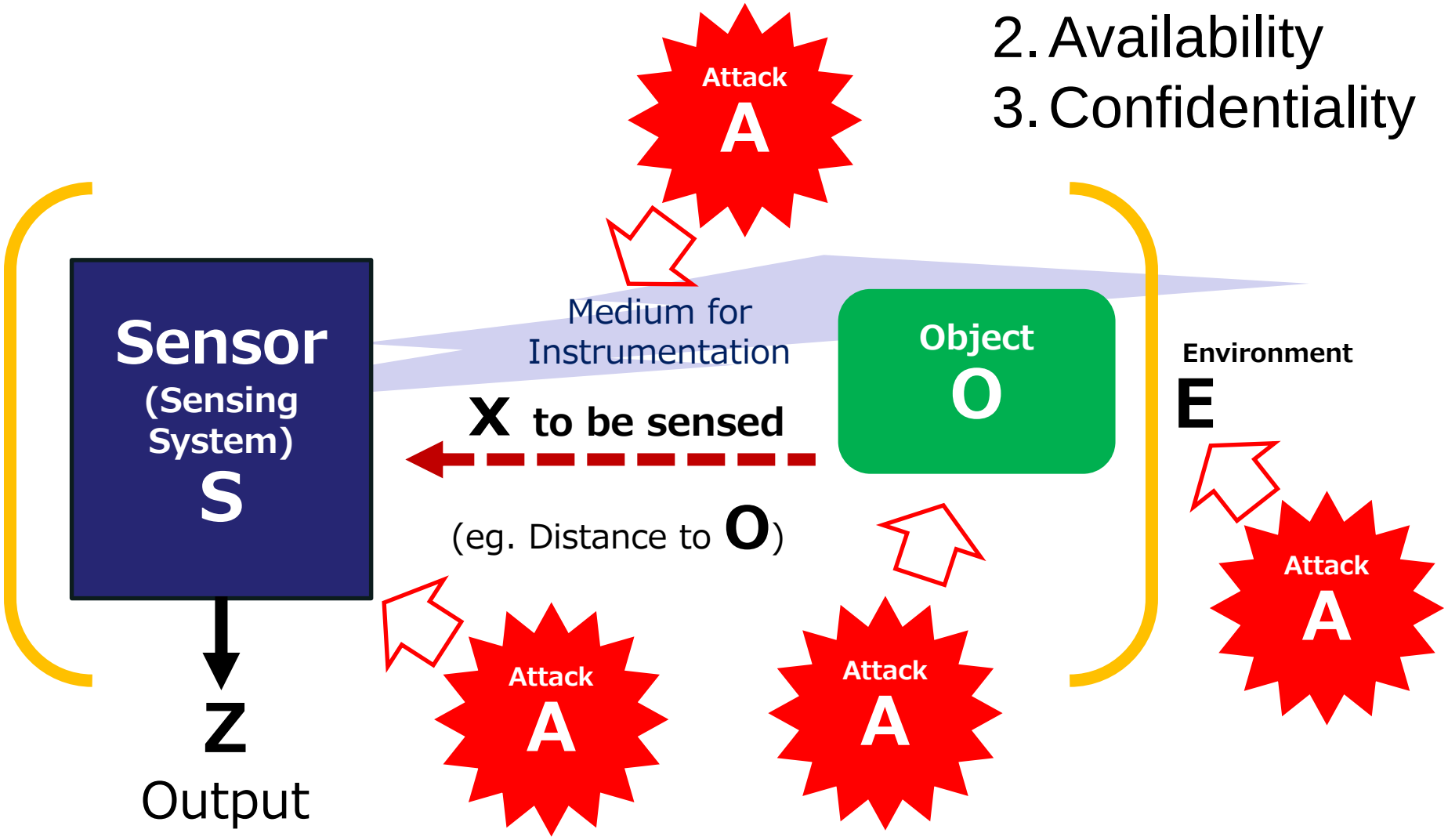
Conventional IPS mainly monitors Behavior of ECUs and Network Traffics. Is it sufficient?

- Anomaly Detection
  - Intrusion Detection System
    - ✓ Host Based/ Network Based
    - ✓ Instrumentation/ Control



Future IDS may cope with
Threats to Instrumentation

Attack to
1. Integrity
2. Availability
3. Confidentiality



Summary

1. A Guideline for Mastering Automotive IDS is desired and being compiled.

2. The Types of Threats that IDS can handle will have to increase.

Tsutomu Matsumoto

YNU YOKOHAMA National University

IAS Institute of Advanced Sciences Yokohama National University