The Session on Cyber Security

Novel Capabilities Required for Intrusion Detection Systems for Automated Driving Vehicles

Tsutomu Matsumoto

Faculty of Environment and Information Sciences
and
Institute of Advanced Sciences

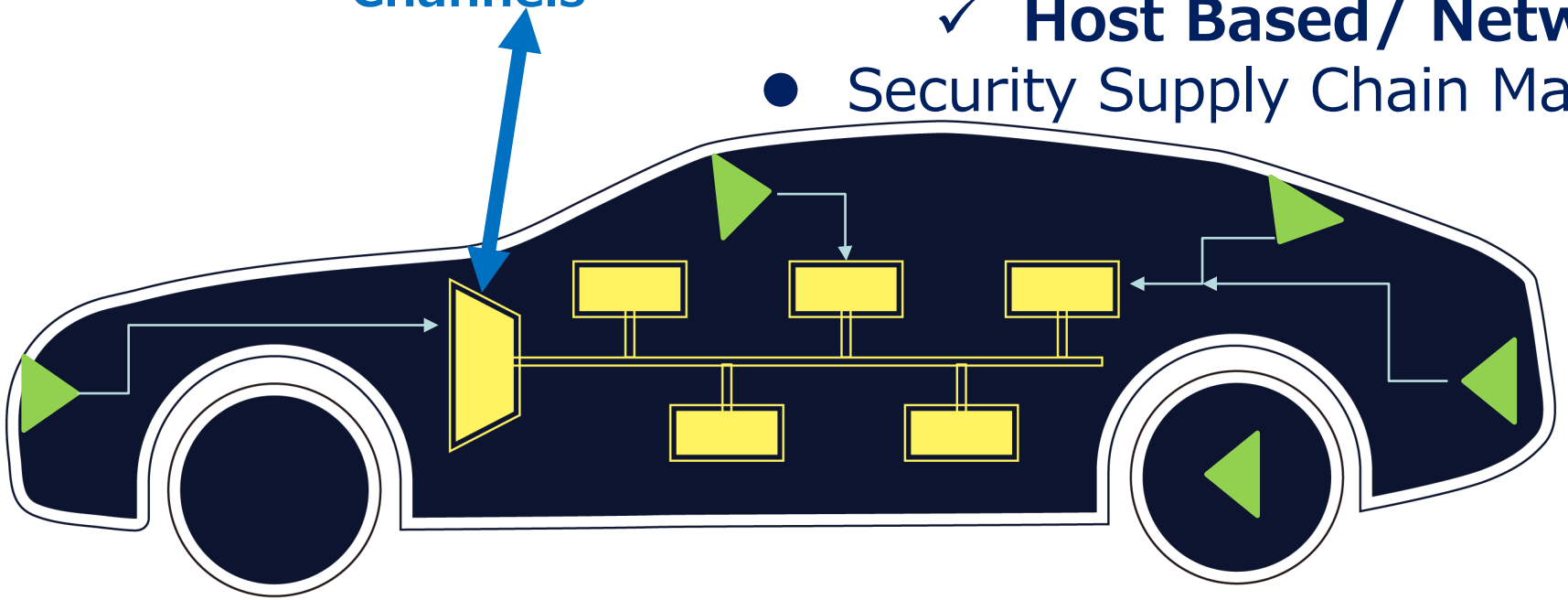
YNU YOKOHAMA National University

Institute of Advanced Sciences
Yokohama National University

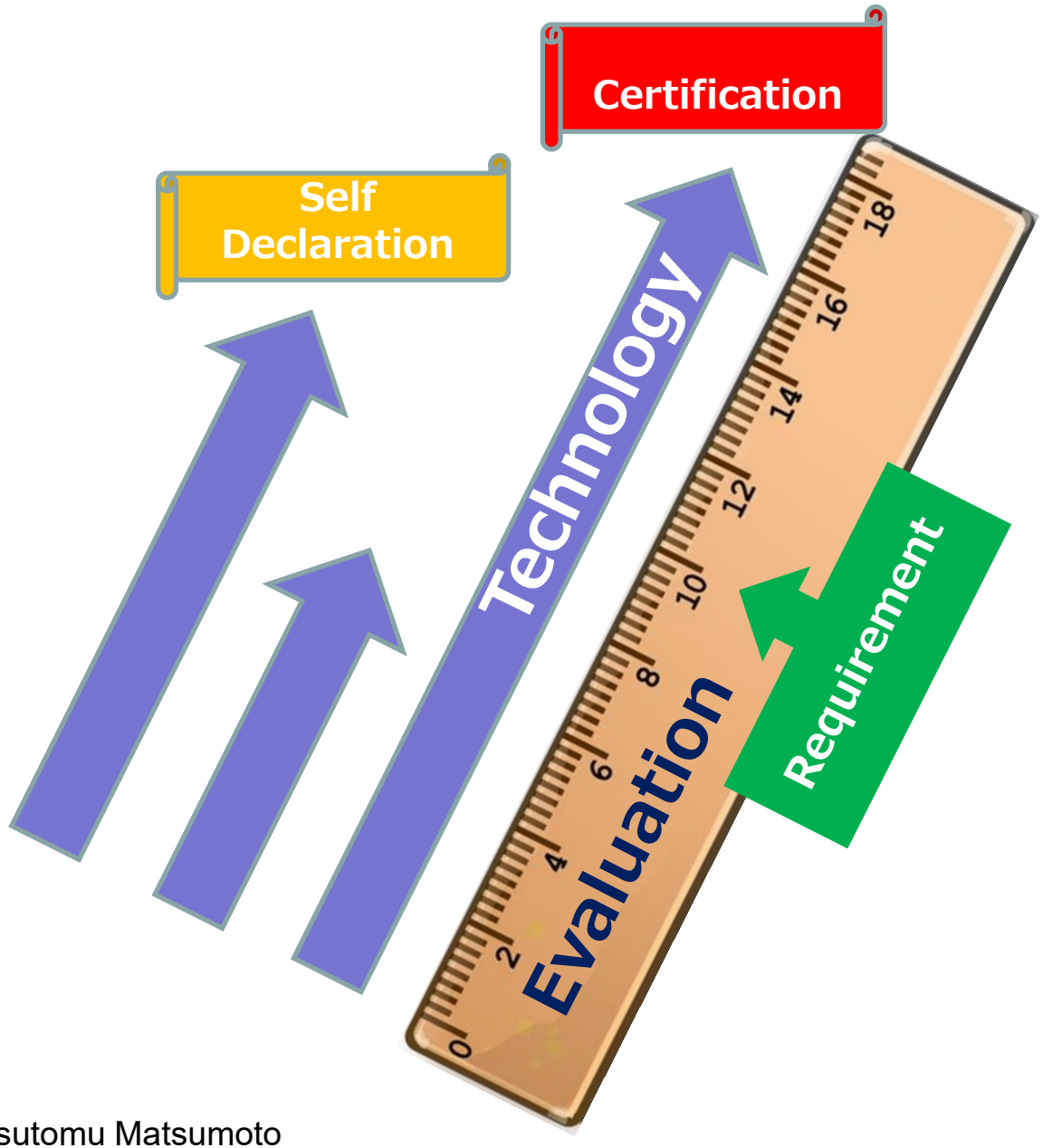
Intrusion Detection System IDS is useful along with other security technologies.

In-Vehicle Network and External Communication Channels

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



Assumptions for Evaluating and Applying IDS

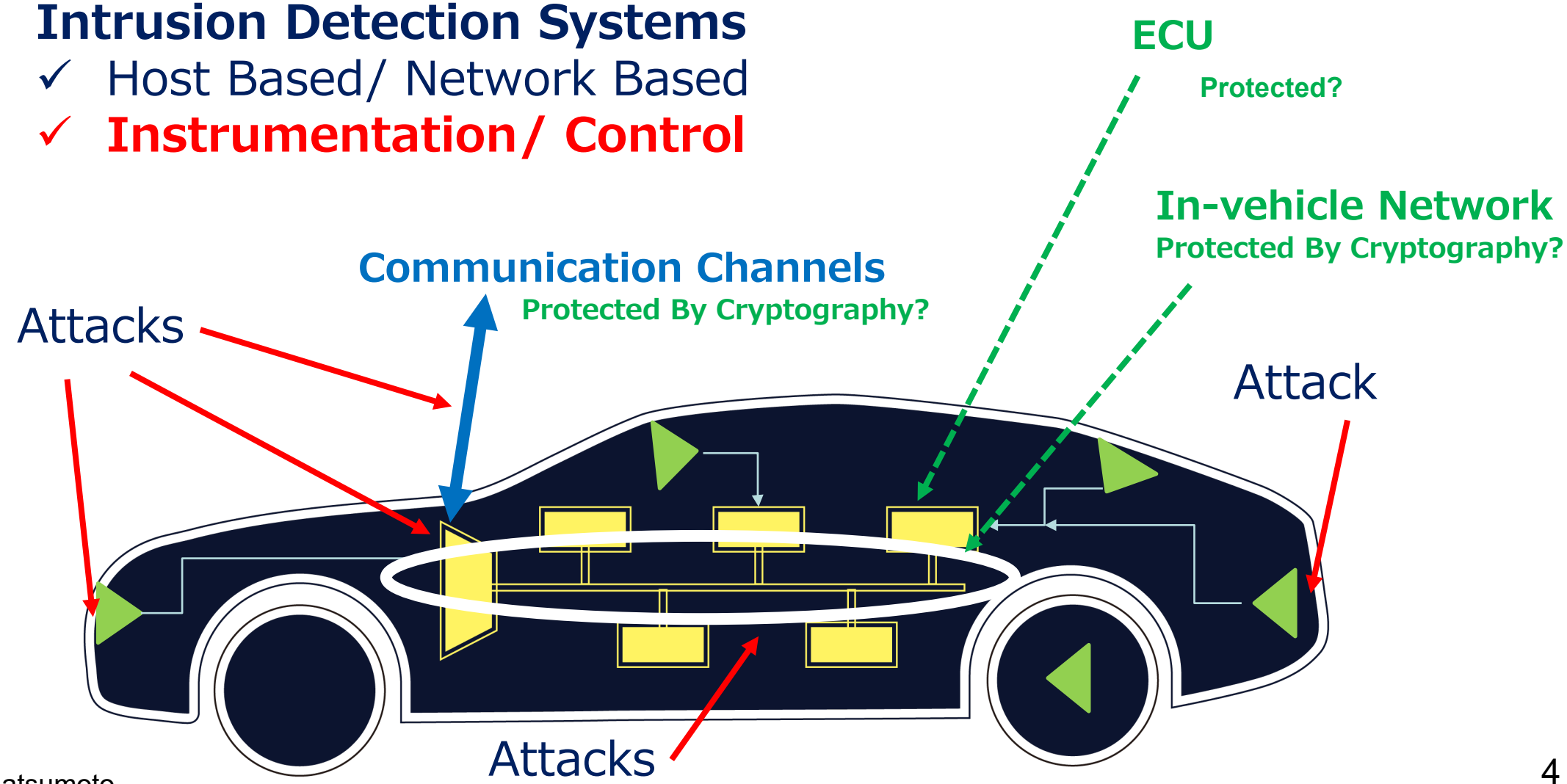


1. Evaluation Technologies and Methods for IDS
2. Technologies to enhance the security performance of IDSs
3. Security Assurance Scheme
   - Self-declaration
   - Third-party certification

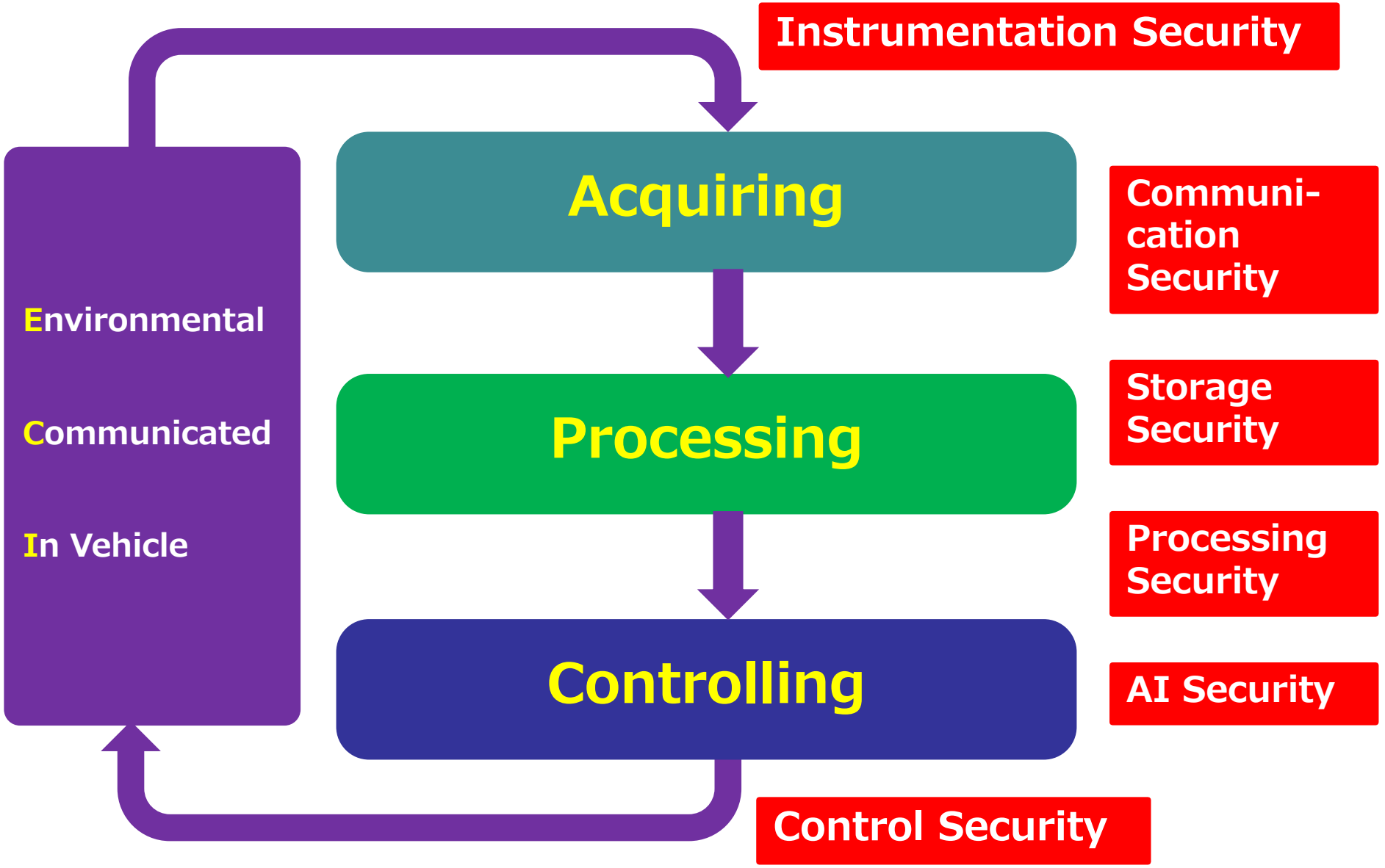
etc. are required to be developed.

Current IDSs mainly monitor the behaviors of ECUs and data on the in-vehicle networks and external communication channels. But are they enough?

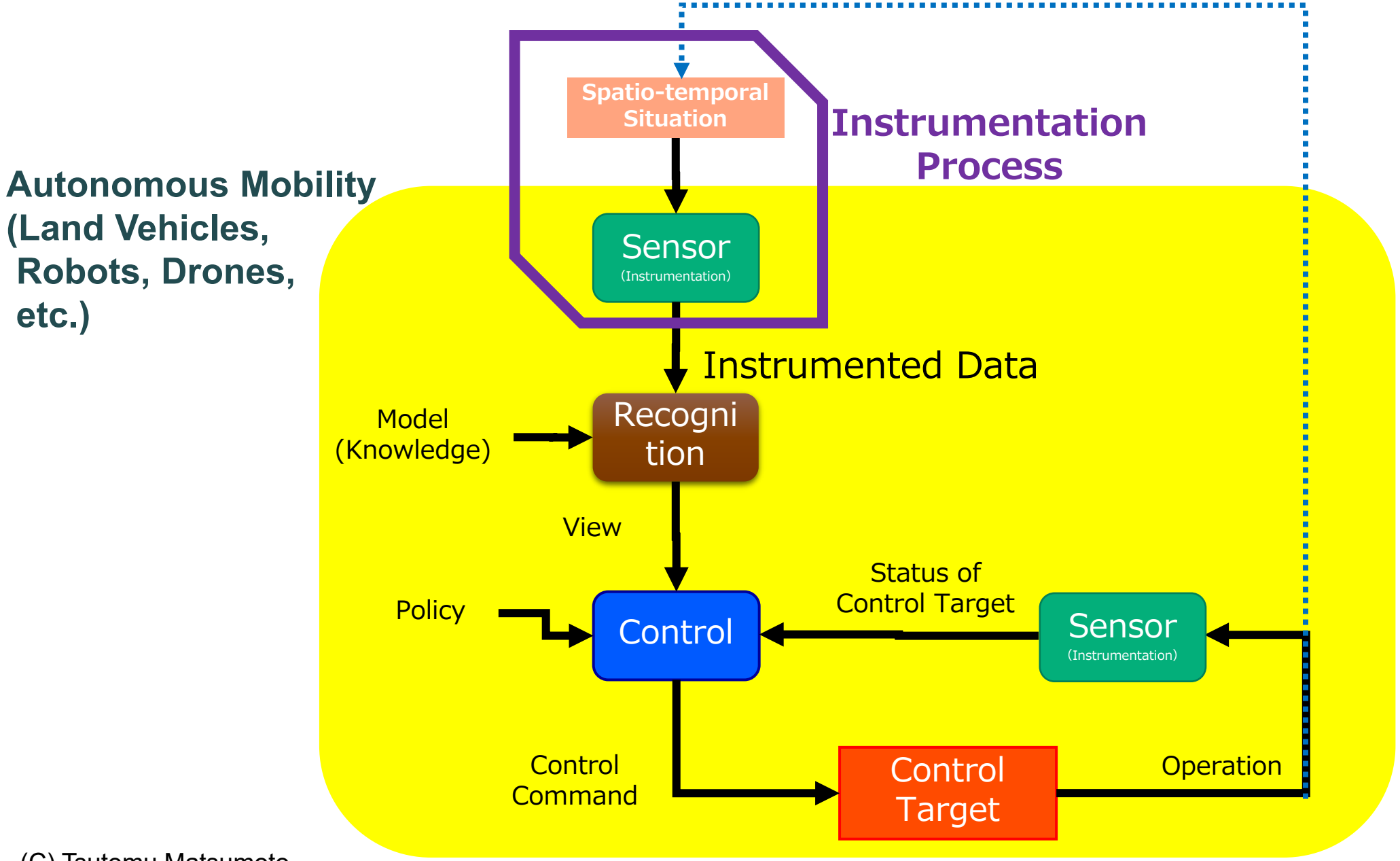
- **Intrusion Detection Systems**
  - ✓ Host Based/ Network Based
  - ✓ **Instrumentation/ Control**



Key Issues in Automotive Cyber-Physical Security

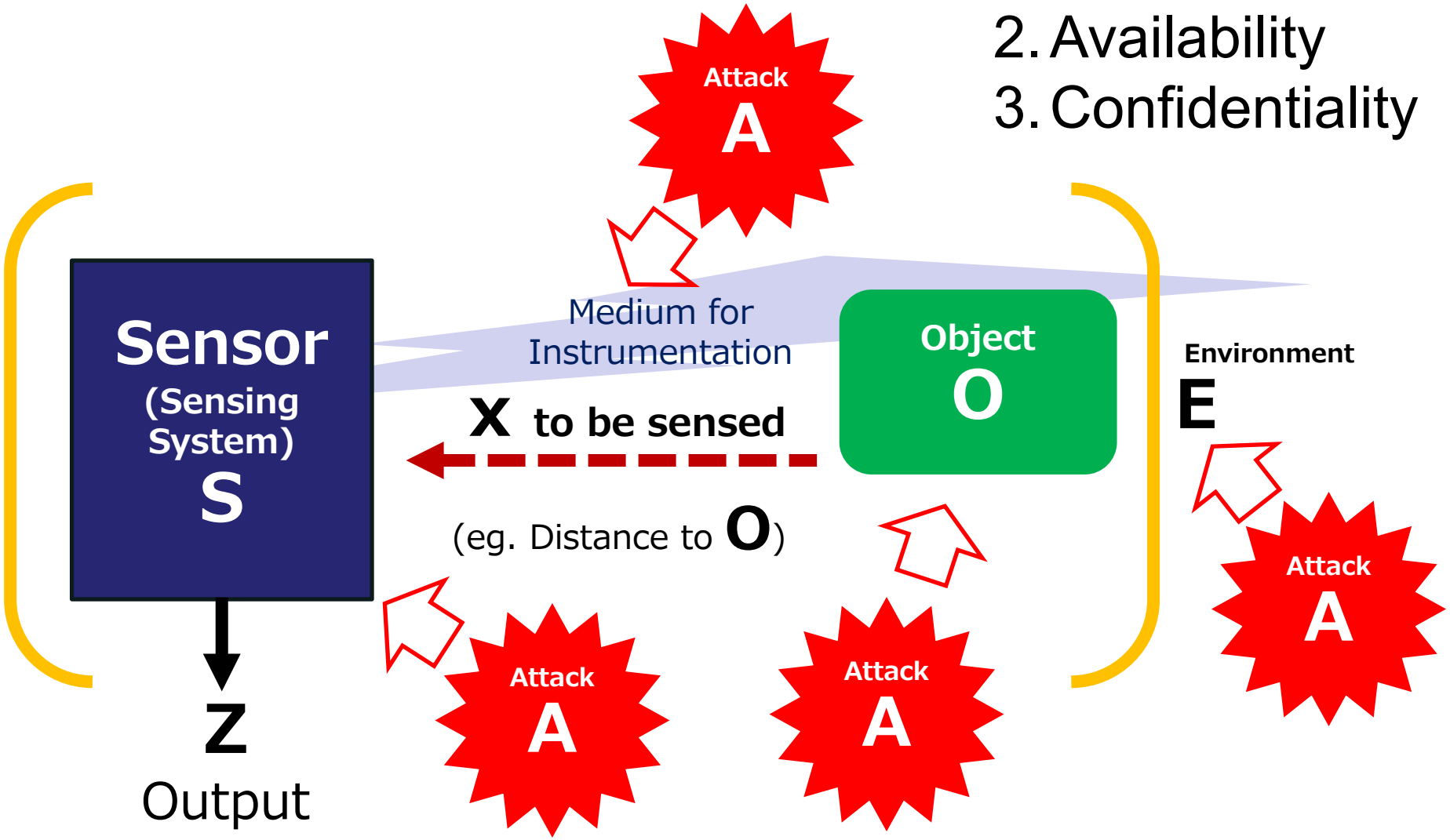


Importance of Instrumentation

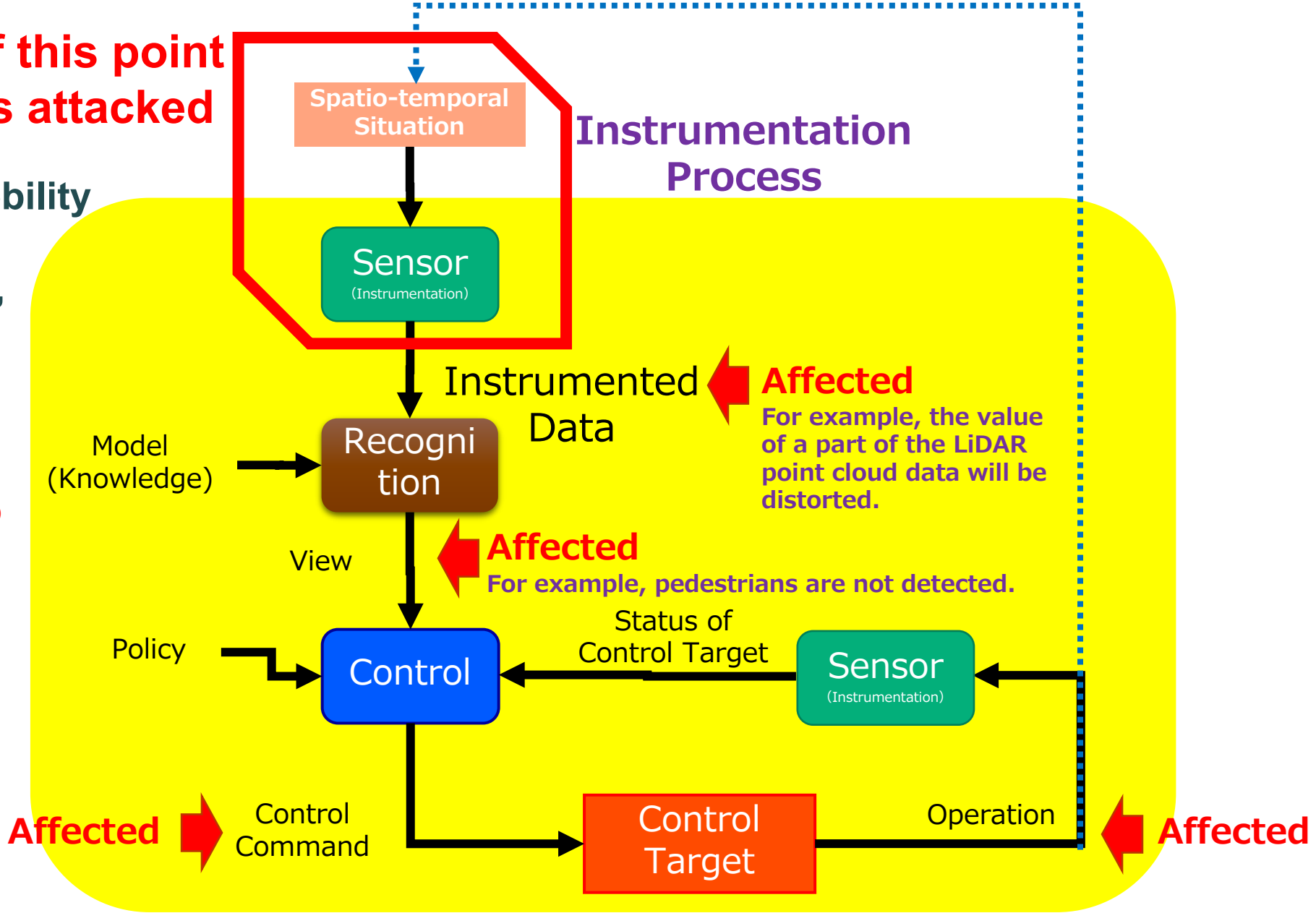


Threats to the Instrumentation Processes

Attack to
1. Integrity
2. Availability
3. Confidentiality



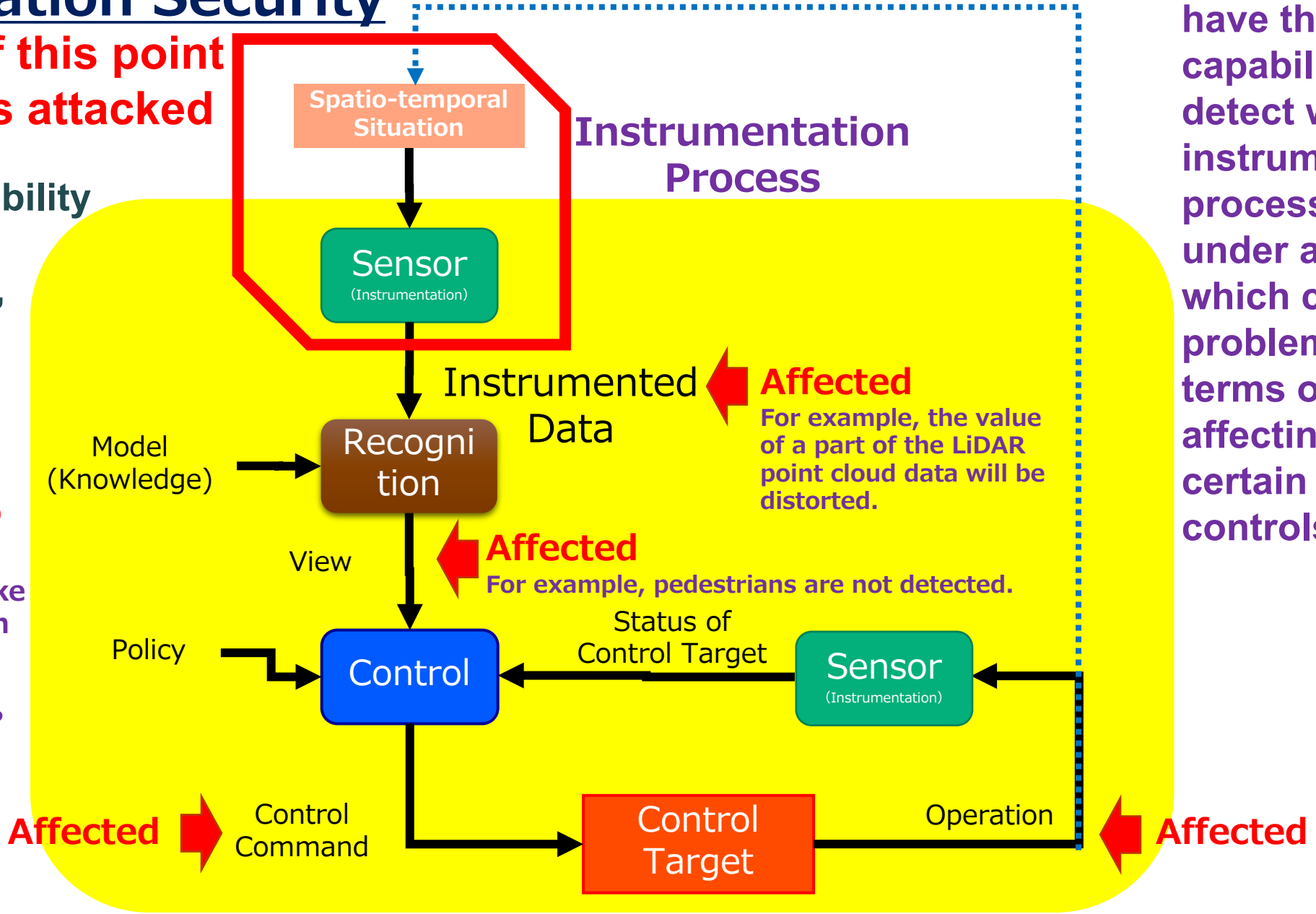
The concept of Instrumentation Security



Autonomous Mobility (Land Vehicles, Robots, Drones, etc.)

Instrumentation Security is directly related to Control Security.

IDS functions required from the perspective of Instrumentation Security



Instrumentation Security is directly related to Control Security.

- Is it possible to make the Instrumentation process capable of detecting itself as being under attack?
- Can we make the Instrumentation process immune to attack?

- An IDS should have the capability to detect when an instrumentation process is under attack, which can be problematic in terms of affecting certain critical controls.

Summary

1. There are a variety of threats to Automated Driving Vehicles: not only threats to ECUs and Networks, but also threats to Sensors and Instrumentation Processes themselves. In other words, there are threats on Instrumentation Security and threats on Control Security.
2. Therefore, the types of threats to be targeted by IDSs for Automated Driving Vehicles may need to be increased in the near future.

ECUs: Detected by behavior

In-vehicle networks and external communication channels: Detected by traffic

Sensors and instrumentation processes: Detected by instrumented data

If you have any questions, please contact Tsutomu Matsumoto at tsutomu@ynu.ac.jp.