| 講演番号 | 165 |
|---|---|

| 文献番号 | 20225165 |
|---|---|

# Autonomous Driving and Cyber Physical Security

**MATSUMOTO Tsutomu**

*Yokohama National University, Faculty of Environment and Information Sciences*
*79-7 Tokiwadai, Hodogaya, Yokohama, 240-8501, Japan (E-mail: tsutomu@ynu.ac.jp)*

**KEY WORDS**: **Information, communication, and control, Combustion analysis,** Cyber Physical Security (E1)

Cyber-physical security for vehicles and operations is essential for the safety of automated driving. This paper provides up-to-date perspectives on how to understand and counter logical and physical intrusions into in-vehicle systems, attacks on measurement, cognition, and decision-making functions based on in-vehicle sensors, attacks on the surrounding environment, attacks on vehicle manufacturing, distribution, and maintenance, and attacks on automated driving operations. In particular, we discuss the perspectives of instrumentation security and control security in detail.

Automated vehicles recognize the spatio-temporal conditions of the surrounding environment based on instrumented data obtained from sensors and models (knowledge) of the instrumented objects and control them according to a policy. The results of control are fed back by sensors that instrument conditions inside the vehicle. The control results also affect the sensors that instrument the surrounding continuum in the form of changes in the spatio-temporal continuum. It is essential to capture various security threats (i.e., attacks) in cyber-physical systems that comprehensively capture the physical and cyber worlds. In particular, we should be concerned with threats that blur the correspondence between things in the physical and cyber worlds. For example, when a self-driving car is instrumenting the spatio-temporal continuum in front of it with a camera or a ranging sensor such as LiDAR, if, due to some attack, a pedestrian who is actually at a certain distance x is measured to be at a much shorter distance n than x, then the self-driving car can brake suddenly or control the steering wheel to avoid colliding with the pedestrian. This could lead to accidents such as rear-end collisions with following vehicles or collisions with guardrails. If a pedestrian is measured to be at a farther distance f than they are, there is a possibility that the driver will make a braking error, resulting in an accident in which the pedestrian is struck. In addition, if the ranging sensor fails to measure the distance, it will not be able to determine the surrounding situation. Any attack on the spatio-temporal continuum or the instrumentation process of a sensor will affect instrumented data, recognition results, and control.

There are various possible ways to modify the spatio-temporal continuum and direct attacks on sensors. How they affect recognition and control depends on how recognition and control algorithms and their implementations are designed. In the past, performance specifications required for sensors were often based on unintentional factors such as noise and disturbances. Still, it has become clear that even small intentional changes or deficiencies in measurements can significantly impact recognition and control, so when considering the effect on recognition and control algorithms, it is crucial to consider the following. We have entered an era in which resistance to attacks on spatio-temporal conditions or sensors should also be considered when defining the performance specifications required of sensors. In particular, it is deemed to be essential to ensure such instrumentation security or control security for Level 4 or higher automated driving.

When designing security, it is essential to construct a security assurance framework. In cyber-physical security, including instrumentation security, the following mechanisms should be established to evaluate the security in each field, specify the necessary security requirement based on the wisdom of the concerned stakeholders, develop security enhancement technologies to achieve the requirement, and apply them in a way that is satisfactory to users. The construction of a new system is required.

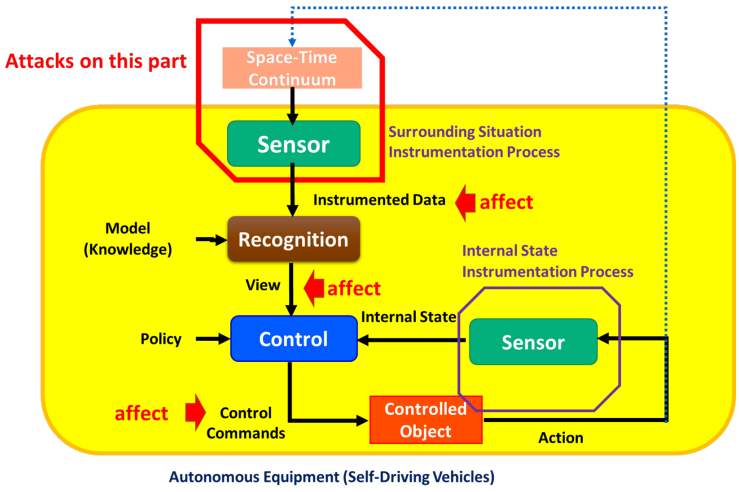


Fig. Instrumentation Security directly relates to Control Security