Towards smooth and safe trading of control from machine to human

Makoto Itoh, Dr., Prof.

Faculty of Engineering, Information and Systems
University of Tsukuba

October 28, 2015

Role of human driver

NITSA's definition of levels of automation

- **Level 0**
  - Manual driving
  - Collision warnings are included.

- **Level 1** ← Current ADAS technology
  - Several control functions are included but they work independently.
  - The driver has overall control responsibility.
  - Either steering control or braking/throttle control but not both.
  - ACC, LKA, Automatic breaking.

- **Level 2** ←NHTSA's primary focus
  - At least two primary control functions designed to work in unison to relieve the driver of control of those functions.
  - The driver is still responsible for monitoring and expected to be available for control at all times and on short notice.

- **Level 3** ←NHTSA's primary focus
  - The driver cedes full control of all safety-critical functions under certain traffic or environmental conditions.
  - This requires transition back to driver control.
  - The driver is expected to be available for occasional control, but with sufficiently comfortable transition time.

- **Level 4**
  - The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for entire trip.

Driver needs to be available when necessary

Issue

- The way of handover from the system to the human driver may be dependent on
  - the reason why the human must takeover the control,
    - E.g. unintended shutdown, failure, noises
  - whether or not there are any remaining functions,
    - E.g. just cruising is available
  - Whether or not the system itself recognizes the necessity,
    - If the system misunderstands the situation, it cannot issues the request for handover
  - whether or not any compensation can be done, and
    - E.g. reducing the vehicle speed
  - the criticality of the situation.

Possible categories of handover

When?	Why?	Remaining function	Can ask driver?	compensation
System shutdown	Explosion, fire, bug, etc	No	no	Not possible
Subsystem shutdown	Sensor/actuator failure, bug, etc	available	Yes	possible
Subsystem inappropriate behavior	Errors in sensor data	Available but inappropriate	Maybe not	Not possible
Subsystem tentatively unavailable	Too much brightness, loss of map, etc.	available	yes	Possible
Beyond system capability	The situation too complex or uncertain	Available but unreliable	Yes	Possible

Trading of Control: From System to Human

Level 2 automated driving.

Sudden heavy fog.
Impossible to continue control.

A. Immediate shutdown

B. Keep control based on the map info only.

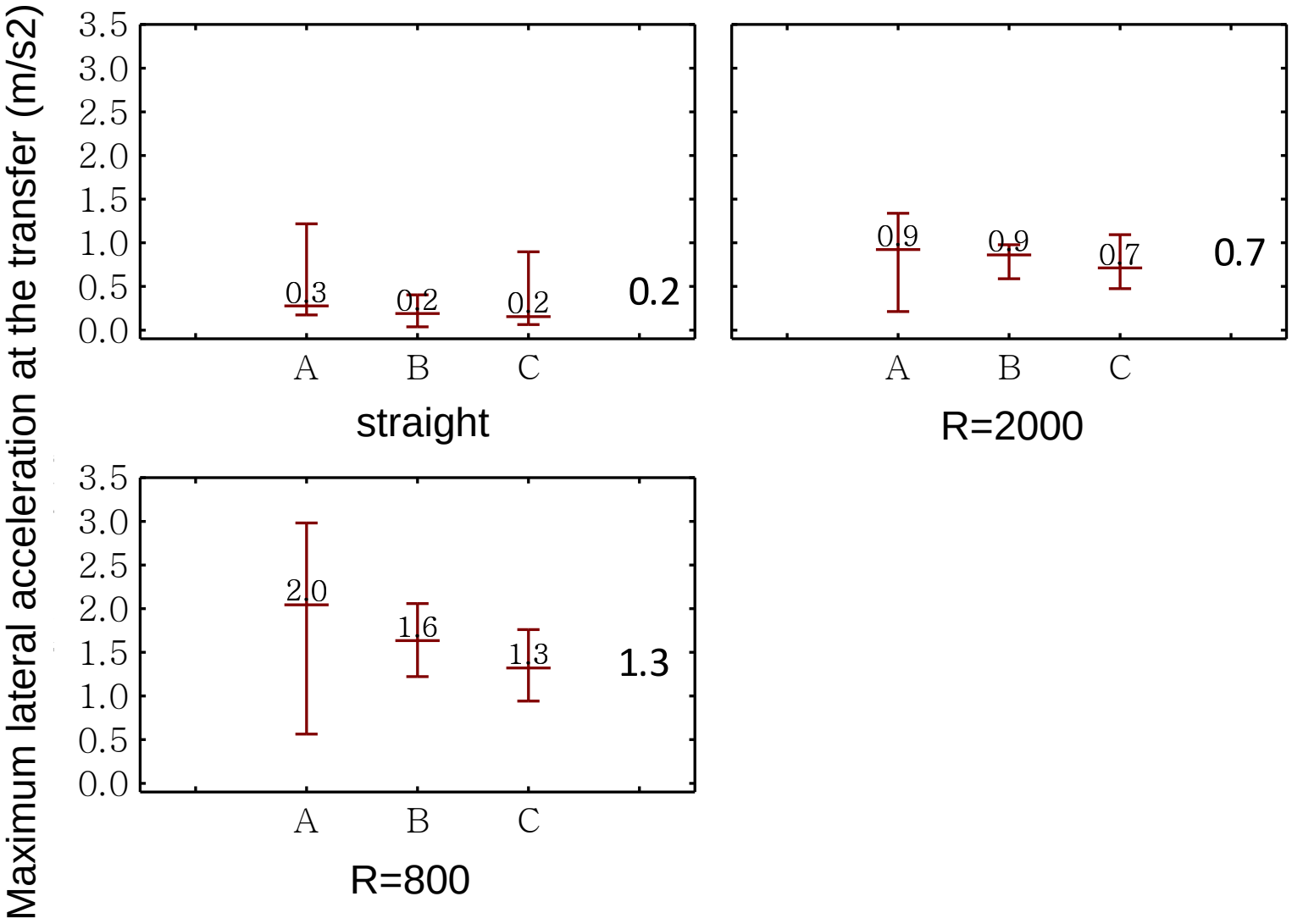
C. Keep control based on the map info only, and reduce the speed.

(Abe, Sato, Uchida, and Itoh, 2015)

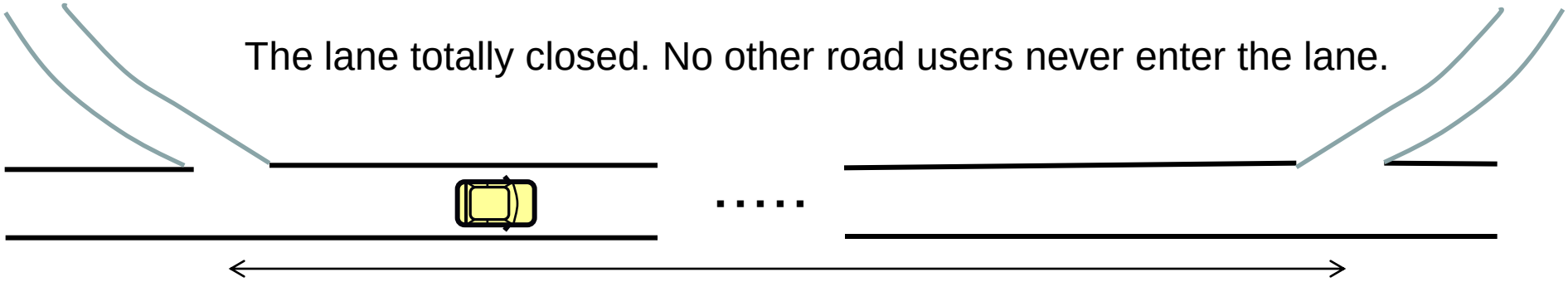
Possible categories of handover

When?	Why?	Remaining function	Can ask driver?	compensation
System shutdown	Explosion, fire, bug, etc	No	no	Not possible
Subsystem shutdown	Sensor/actuator failure, bug, etc	available	Yes	possible
Subsystem inappropriate behavior	Errors in sensor data	Available but inappropriate	Maybe not	Not possible
Subsystem tentatively unavailable	Too much brightness, loss of map, etc.	available	yes	Possible
Beyond system capability	The situation too complex or uncertain	Available but unreliable	Yes	Possible

Results: Types B and C would be better for smooth handover



Automated driving only on dedicated lane

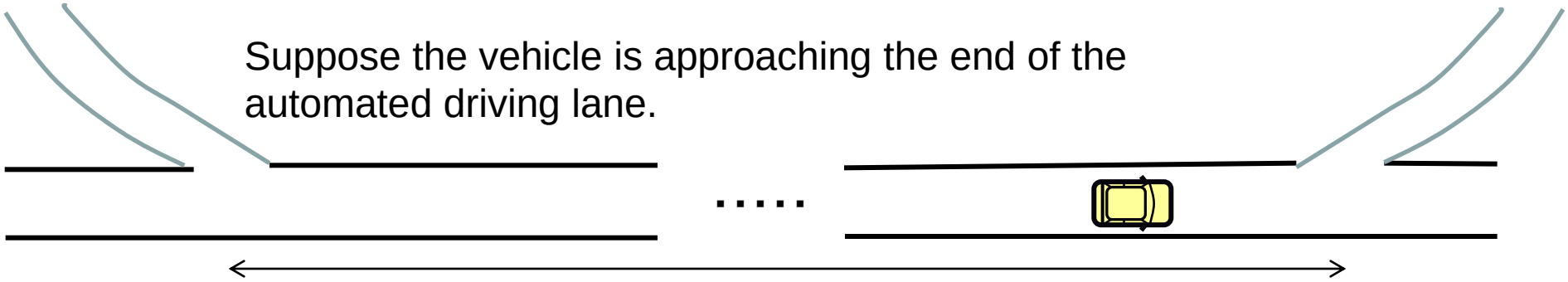


Level 3 automated driving, but under quite limited conditions.

The automated driving system may not be so intelligent to understand the behaviors and intention of other vehicles.
- the map
- the location and speed of the surrounding vehicles, etc.

The system may be unavailable when
- the vehicle goes beyond the dedicated lane,
- the visibility is too low due to fog etc.

Automated driving only on dedicated lane (cont'd)



The automated driving system can identify where to hand over the control.

If the driver does not respond at all, the system may reduce the speed or stop at some point.

That is, the time requirement can be changed. It is not necessary to answer the question "how many seconds the driver needs to recover."

Possible categories of handover

When?	Why?	Remaining function	Can ask driver?	compensation
System shutdown	Explosion, fire, bug, etc	No	no	Not possible
Subsystem shutdown	Sensor/actuator failure, bug, etc	available	Yes	possible
Subsystem inappropriate behavior	Errors in sensor data	Available but inappropriate	Maybe not	Not possible
Subsystem tentatively unavailable	Too much brightness, loss of map, etc.	available	yes	Possible
Beyond system capability	The situation too complex or uncertain	Available but unreliable	Yes	Possible

The question

- Critical issue on Level 3 automated driving.

How many seconds will be needed for the handover?

- We could answer the minimum value (or necessity condition) to the question, but not the sufficient condition.