SAFER

VEHICLE AND TRAFFIC SAFETY CENTRE AT CHALMERS

Facilitating Joint Analysis of Data from Different Projects and Countries

Trent Victor, PhD

Volvo Technology/ SAFER,

SHRP2 Safety Symposium

Washington, DC, 2009-07-22

Goals

- A SHRP2 goal is to encourage data sharing and comparative research/analysis of SHRP2 and other country data.
- Joint analysis vs data sharing
  - Options:
    1. Perform similar/standardized analyses (e.g. HASTE)
    2. Give out aggregated data (e.g. EuroFOT)
    3. Give out well-identified sections of data only
    4. Give out all/some pre-processed data with explanations
    5. Give out all/some raw data

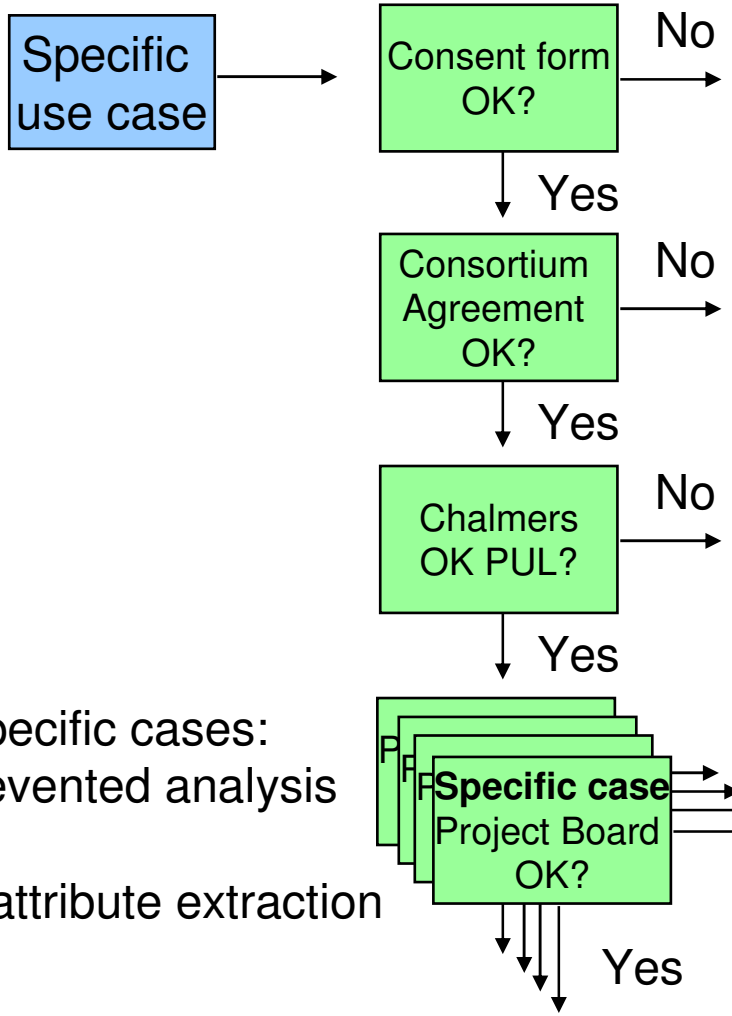
Challenges

- **Data categories**
  - Open, OEM-shared, etc
  - Be specific when talking about CAN data (it's like USB/LAN)
- **Data ownership**
- **Utilization rights**
  - During and after project for which purposes for which partners (e.g. handling 3rd parties)
  - Who has disclosure rights, what approval process?
- **Legal and Liability issues**
- **Ethical and Privacy issues** – youtube anonymous
- **Proprietary data issues** (e.g. OEM/supplier concerns)
    - Reverse engineering of new/unique systems (active safety systems)
    - Public exposure of faults with systems
    - Existing 3rd party agreements (e.g. suppliers) may prohibit sharing data

SeMiFOT Access and Ownership Scheme

• Questionnaires- and interview data • Video • GPS • Mounted sensors (eyetracker, lanetracker, headway, etc) • CAN-data – Open CAN (y) e.g. speed, steering angle, accelerometers, yaw, pedal use, blinkers, wipers, temps, etc	Open access to all project partners Owned by all project partners Located at SAFER
– Closed CAN (x) but shared for specific purposes between OEMs and institues	Access by sub-sets of partners Owned by the respective OEMs Located at SAFER (controlled access)
– OEM-specifc CAN (z)	Access limited to OEM Owned by OEM Located at OEM

Exception handling – Unforseen use of data from SeMiFOT dB



-Driver consent

-Third party approved by OEM and Chalmers
-Common x-analysis at SAFER

-Inform on new data types
Analysis at SAFER

Examples of specific cases:

1. Events-prevented analysis at UMTRI
2. Map data attribute extraction

Main rule:
Analysis at SAFER and OEM Premises

Data used elsewhere only in selected specific cases

Data Security – Main Threats Identified

1. Personal data (mainly video data) becomes public, through for example publishing on internet.
2. Loss of - or manipulation of data
3. Confidential information becomes available for competitors
4. Legal violations by video recording at places where recording is prohibit
5. The research data will not get adequate secrecy protection – physical workspace requirements, isolated computers are difficult, database administration, etc