Forensics - how do we know what the problem was and how the system reacted?

World café session at the "Safety assurance and managing risk in automated driving" SCSSS workshop 2018

-

Brief summary from discussion rounds (by Martin Törngren, KTH)

Forensics world cafe table

Some considerations and questions that were put forward to initiate the discussions:

- Complex traffic scenarios and connected transportation systems
  - distributed state information
  - Difficult to collect digital evidence and reconstruct activities (answering what, where, when, who, why and how)
- How to understand (re-construct/re-create) the actual scenario that lead to an accident/incident?
  - External events? Internal events? Level of Intrusiveness /access to internal states
- How to understand what actually caused the accident/incident – and how far back should one go?
- Further considerations for gathering the data, how to trust it? Security attacks, integrity of data.

Summary from forensics world cafe table discussions

A number of topics were touched upon during the 4 rounds, including the following, that are briefly summarized in the following slides

- The role of regulations and standards
- Best practices in other domains
- Current practices and limitations
- What to store, storage capacities, sources
- Driving standards and data sharing forward
  - Data ownership

The summary represents statements by the various participants in the four rounds for this table.

The role of regulations and standards

- The Automotive domain has generally few regulations compared to other domains
  - No centralized authority as for aerospace and medtech
- For trucks, “tachografs” are regulated and mandate recording certain data
  - This could be something to build upon towards “black boxes”
- Regulations referring to integrity and privacy of data, constrain what data that can be captured and stored; this also varies among countries. For example, camera data may be sensitive in Europe, but allowed in some asian countries
  - E.g. what about cameras capturing the road side and houses?
- Mentioned by a participant: The ISO26262 is in place because authorities told the automotive industry they had to provide a standard
- A standard for black-box logging should be relevant for future complex cars – there is a need to learn from accidents and to accelerate learning across multiple companies

Best practices in other domains

- In domains such as Aerospace, Trains and MedTech, black boxes are mandated since many years and has explicit use in forensics!
- The tasks and data to record by the black boxes are defined through international standards, specifying e.g. what data to record and with what frequency
- Sometimes the standards are seen as limiting, e.g. the mandated frequency may be too low for detailed analysis
- A typical practice was mentioned from aerospace, to record 30s windows that are then overwritten
- The culture of forensics from the aircraft industry was highlighted; that of **not** attributing blame during the analysis, in order to better be able to find the “root cause” and to learn to improve practices

Current practices and limitations

- No regulated black boxes, but
- Car manufacturers do have some internal (own initiated) recording
  - Example was mentioned for active safety such as emergency braking to record internal states.
  - This is likely to evolve and consider the many sensors that are fitted for automated driving
- Current vehicles have limited on-board storage

What to store, storage capacities, data sources

- To reconstruct what happened – what data needs to be stored?
  - Raw data? Abstract filtered data? Decisions? Frequency of sampling?
  - How to capture the traffic environment?
  - Raw data from e.g. cameras produce large amounts of data
- The interpretation of data may benefit from use of other data. Perhaps vehicles could be seen and used as witnesses – asked to store relevant data. This will require agreements and communications. Data may also be recorded by the infrastructure
- If data from multiple sources (e.g. vehicles) is to be collected and used, relating data through e.g. time stamps will be needed (possibly through GPS);
- It was generally agreed in the discussions that a combination of short and long term data storage appears relevant, with key events stored long term, and a suitable short term buffer that is continuously overwritten. Significant events need to be defined, e.g. map updates!!
- Who owns the data needs to be considered. This might change in the case of an accident. For example, it was mentioned that for a “crime scene in the UK” this means automatically that ownership is transferred to authorities

Driving standards and data sharing forward

- In summary, the participants appeared to agree that there is a need for a standard for black-box logging considering the complexity and novelty of automated driving. There is a need to learn from accidents and to accelerate learning across multiple companies
  - Sharing incident info across brands like in aerospace
- Doing this type of standardization will however be non-trivial giving the ongoing technological development and the heterogeneity of data sources.
  - Nevertheless important to get started to evaluate and learn, a careful - stepwise introduction was suggested
- The interest of insurance companies in logging data was mentioned, and their intent to incentivize behaviors that lower risks