Cooperative advanced driver assistance systems

Technological measures for data privacy compliance

Informational self-determination, digital signature, Car-to-X communication, Big Data analysis

Cooperative advanced driver assistance systems (ADAS) will contribute to road traffic safety: Critical situations will be detected, the driver alerted and control of the vehicle interfered with automatically. However, the introduction of such driver assistance systems presupposes that data privacy issues have already been solved in advance. A necessary condition for the driver to accept and trust new driver assistance systems is that his/her personal and personally identifiable data will be treated with a high level of integrity.

Authors: Hubert Jaeger, Lars Schnieder

This article presents an approach to maintaining a high level of integrity in dealing with this data.

Weighting rivaling legal interests

Technological implementation of cooperative advanced driver assistance systems (ADAS) reveals two rivaling legal interests:

1. The protective effect of active safety systems and, accordingly, the individual right to life and physical integrity (see EU Charter of Fundamental Rights)
2. The right to informational self-determination (see EU Charter of Fundamental Rights)

Protective effect of ADAS

The United Nations' Decade of Action for Road Safety campaign goal is to reduce traffic accidents worldwide by 50 % by 2020. Reaching or even exceeding this target (i.e. "Vision Zero"), requires a comprehensive integrated traffic safety work plan (Ahrens, et al., 2010). Advanced driver assistance systems play a major role in achieving this objective. Ahrens distinguishes three different levels of ADAS:

1. Systems that recognize a vehicle's movement and compare it with the driver's intentions (anti-lock braking systems)
2. Systems that additionally use environment-related data provided by the vehicle's sensors (lane keeping assistance systems, LKAS)
3. Systems whose sensors also provide the vehicle with otherwise inaccessible information (front collision warning systems, FCWS) (Franke, et al., 2013)

Vehicle-to-vehicle and vehicle-to-infrastructure (V2I) communication will allow all motorists to "cooperate" (Köster, 2014). This will improve traffic flow and increase traffic safety.

Right to informational self-determination

Dedicated Short Range Communication (DSRC) according to ETSI ITS G5 standards sends information on traffic light signal times or existent traffic regulations (e.g. speed limits). Besides merely transferring data for the respective use cases, it is essential that deliberate falsification or manipulation of the signals sent be prevented. As a basic principle all vehicles and traffic light control units need to be protected against manipulative information and any kind of attacks. *Figure 1* illustrates intelligent traffic system attack vectors. Said protection should comply with process and technical specification defined per international standards for programmable traffic control and surveillance application system development (DIN, 2008) and functional road vehicle safety (ISO, 2011).

Technical solutions are based on systems in which outgoing communication is equipped with a digital signature, the validity of which is verified on the recipient side. This requires taking technical and organizational measures for certification and, in case of doubt, revocation of the same. Current communication protocol specifies cyclic codes for cooperative advanced driver assistance systems use cases (Köster, 2014). The cooperative ADAS transmits said codes, which categorically include personally identifiable information (i. e. vehicle ID) at intervals of a few seconds as well as use-case-relevant parameters, such as speed, direction and location of the motorist:

- Cooperative Awareness Messages (CAMs) convey information on the presence, whereabouts, speed, sensor data and current status of communicating, neighboring ITS stations. These are used for instance to warn drivers of potential collisions at intersections.
- Decentralized Environmental Notification Messages (DENMs) send situation-specific local hazard warnings (Franke, et al., 2013). A typical use case is a road hazard warning, which consists of multiple applications.

The data sent from ITS station to ITS station is not only applicable to the initially intended purpose of driver assistance. This data may also be used for tasks of public authorities, e.g. authorized criminal investigation or prosecution of speed limit violations or similar (Rannenberg, 2015). This allows driver profiles or "digital traffic tickets" to be issued. On the one hand, digital signatures enable authentication. On the other hand, they represent personal and personally identifiable data or much less distinguishing marks that can potentially reveal a communication partner's identity. Consequently, from the point of view of privacy legislation, communication of car-identifying signatures of the transmitted messages should be viewed critically. After all, such administrative interference with the right to informational self-determination requires a purpose or basis for author-

ity regulated by law, i.e. an enabling provision (Kost, et al., 2013).

Privacy law framework

Advanced driver assistance systems support and inform the drivers and increasingly relieve them of certain tasks. According to Bendel (2014), this raises information ethics questions. Personal rights and interests should be understood, respected and observed when information technology is applied. Information ethics groups emphasize the importance of protecting and preserving informational autonomy under ADAS. Accordingly, ethical standards have been set out in writing in relevant legal standards and legislation (e.g. Directive 95/46/EC). Each individual has the right to command and determine their own personally identifiable data. Since implementing and using intelligent traffic system (ITS) applications and services implies processing personally identifiable data (EU, 2010), protecting data privacy interests is imperative.

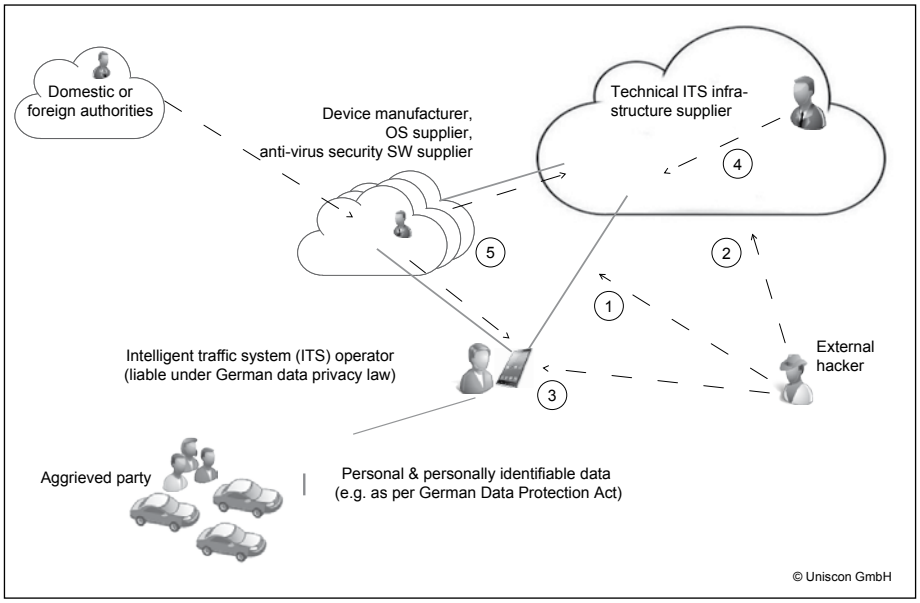

Figure 1: Intelligent traffic system (ITS) attack vectors

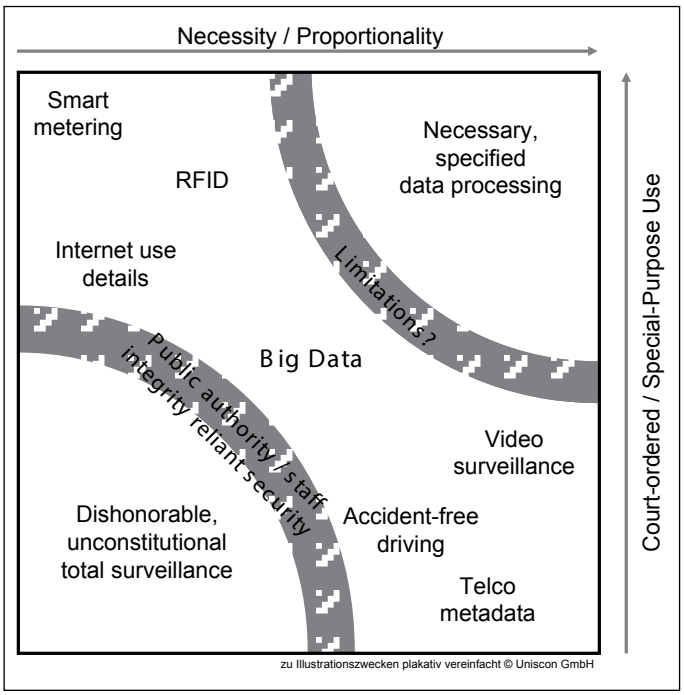

Figure 2: The special-purpose and proportionality challenge

Principle of proportionality

The latter also means that any action of the authorities must remain commensurable and observe the principle of proportionality. This rule of law ("prohibition of disproportionate measures") is statutory and for example laid down in the German Constitution. "Proportionate" (i.e. commensurate) implies that any action taken by the authorities must be *appropriate*, *necessary* and *reasonable* as to the purpose to be served (Keil, 2014). A measure is defined as *appropriate* if it serves to achieve the set objective. It is considered "*necessary*" if deemed the "mildest" of all adequate measures and "*reasonable*" if and when proportionate with the objective pursued. Consequently, EU ITS Directives (EU, 2010) stipulate that personal and personally identifiable data may merely be processed if and when necessary for ITS application and service operation.

Principle of special-purpose use

The principle of special-purpose use pursuant to the relevant EU Directive (EU, 2010) is also valid for ITS applications. The mentioned principle indicates that the right to informational self-determination may merely be restricted to the "inevitable". The special-purpose principle stipulates that the acquisition, use and storage of personally identifiable data may only be ascertained for specifically defined, explicit legitimate purposes. Moreover, further processing (i.e. use, modification, linkage and storage) of personal data is only admissible to the extent that it remains reconcilable with the respective special purpose (Rannenberg, 2015). The period and amount of data that may be processed is strictly limited to the amount needed to achieve the given objective (Keil, 2014) (Douma et al., 2012).

Resulting challenges for privacy-compliant Big Data analysis

The aforementioned elementary principles of proportionality and special-purpose use span the fields of activity shown in *figure 2*. As shown in the bottom left corner, in the worst-case neither objective is achieved. At best (top right), both objectives are fulfilled. However, the party amenable to law (the official investigative authority) must comply with the data subject's rights. The person concerned must be informed, has the right to delete or block data, and the right to objection (Douma et al., 2012). Compliance with regulations concerning the data subject's consent to processing of personal data (EU, 2010) must also be observed, provided that there is no legitimate purpose regulated by law. In cases where a large quantity of data is consolidated, a specific explanation as to its purpose and processing or use is required. If the data subject does not effectively consent to the processing and use of his/her data, so-called "reasonable initial suspicion" postulates the existence of at least "sufficient actual" evidence, to be able to presume a criminal offence or misdemeanor.

According to the European Court of Justice (ECJ), storage of Big Data is irreconcilable with the EU Charter of Fundamental Rights. Also the German Federal Constitutional Court's First Senate has declared data retention to be altogether "unconstitutional and null and void by law", ordering that data stored to date be deleted with immediate effect. In its court opinion the court frames material, organizational and procedural specifications regarding data storage, transfer and usage: It must be assured that security standards reflect the technical discussion's development, continuously incorporate the latest scientific findings and insights, and are not subject to the free weighing of economic interests (Federal Constitutional Court decision dated 3/2/2010, 1 BvR 256/08).

In the following, we introduce a technology that ensures the protection of the authorities' interests pertaining to the aforementioned legal principles.

Sealed Freeze and Sealed Analytics solutions

Both technical solutions, Sealed Freeze (data-privacy-compliant data retention) and Sealed Analytics (compliant Big Data) are based on the fact that the potential of Big Data may only be used if any risk of uncontrolled data distribution and data abuse is eliminated. A combination of intelligent technologies, updated applicable law and technical regulations can ensure this. The data privacy technology mentioned herein allows performing Big Data analyses while maintaining a high level of integrity when dealing with personally identifiable data (Rieken, et al., 2015).

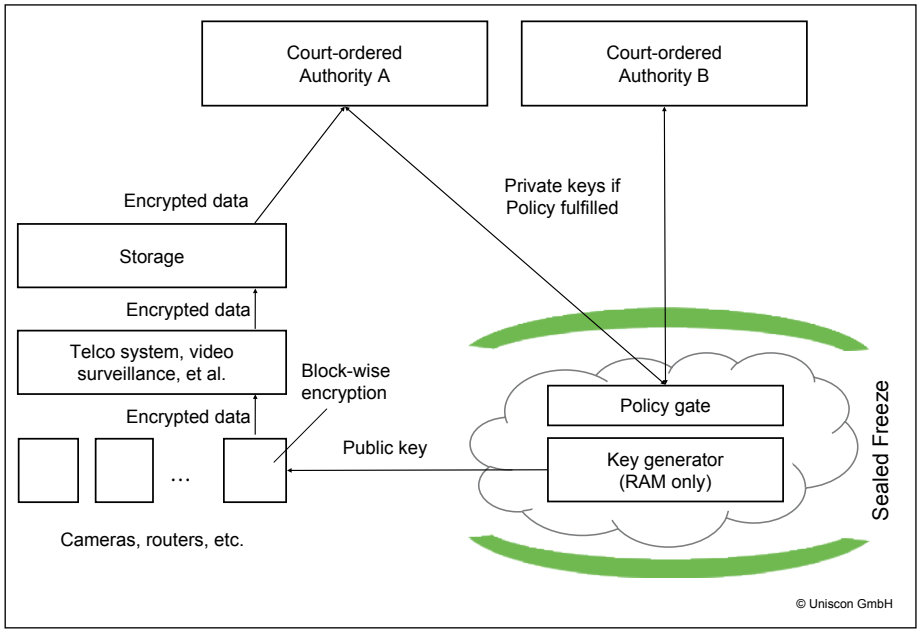

Figure 3: Sealed Freeze application components

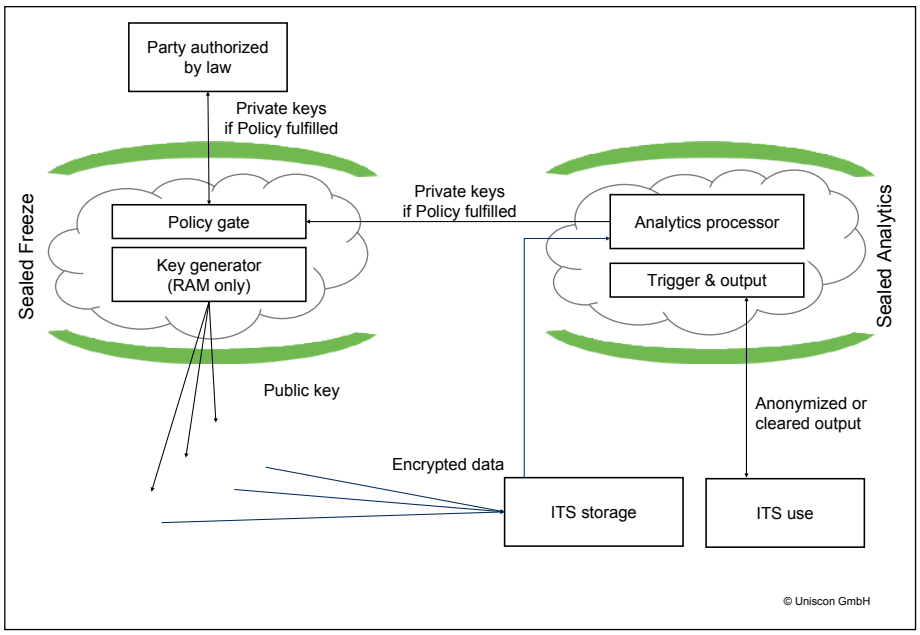

Figure 4: Privacy compliance for Big Data via Sealed Analytics

Storage in a sealed environment

The sealing technology is based on the fact that only specifically defined and technically verifiable parties can access data. Access control specifies who may work with personally identifiable data to what extent. Since provider staff cannot access Sealed Cloud data at any time (Jäger et al., 2013), a "key generator" is necessary to create a vast amount of asymmetrical pairs of keys. Public keys can then be exported to where the data is collected, in order to encrypt the data block-wise. Private keys, which are necessary for decryption, are stored per multi-redundant, yet (merely volatile) random-access memory (RAM) within the Sealed Cloud. This type of storage ensures, via Sealed Cloud security, that no one can access unencrypted storage data, neither per authorized nor per unauthorized access. Planned access, e.g. during maintenance, or unplanned access, such as cyber attacks, triggers an alarm and automatic data clean-up.

Sealed Freeze and Sealed Analytics access per policy gate

The core characteristic of the technology is that access to data stored in this manner is granted technically, i.e. by a set of fixed rules (policy) specified in advance (Kost, et al., 2013). Said policies are subject to data privacy specification. Consequently, differing individual policies may be created for Big Data. These are subject to a three-layer formula:

- The first level of protection fulfils the minimum legal requirements of data privacy law.
- The second level includes supplementary data privacy specifications covenanted with the user.
- The third level of protection is a particularly commendable example of implementation of the principles of data privacy, e.g. in terms of data austerity or privacy by design (Douma, et al., 2012).

A judicial decision, i. e. court order, is the condition precedent for a person to be authorized access to personal or personally identifiable data. Client certificates can verify an authorized party's identity with certainty, since they are allocated to specific devices. If an authorized party must access personal data or metadata for investigative

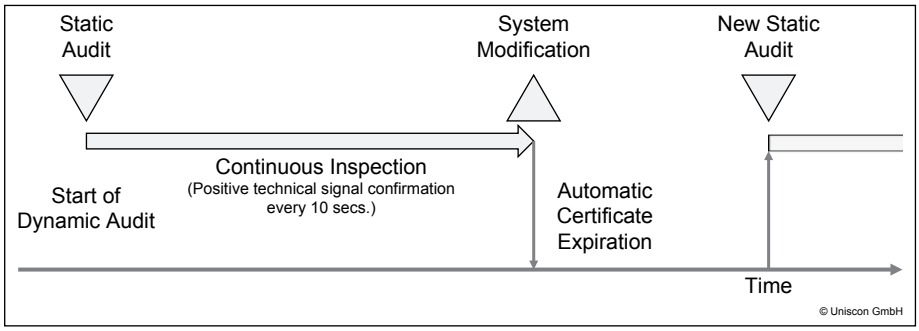

Figure 5: Dynamic audit

purposes, then this is merely feasible via policy gate. The policy gate implements a logic that is strictly modifiable for versioning only. Reverse modification of the logic is impossible. *Figure 3* illustrates the aforementioned Sealed Freeze components.

Sealed Analytics

Sealed Analytics technology is based on the above principle and enables specific, court-ordered analysis of data, provided that the corresponding semantics are allocated prior to storage and a set of metadata has been accumulated. Accordingly, specific rights allocation allows authorized parties access to specific data. Said authorized parties are also only granted access to personally identifiable data that is needed to perform the respective task. Up-front policy specification allows access criteria to be defined individually. For example, access might be granted for specific data types only, or limited periods of time, limited data volumes, and specific types of traffic or usage rights. Any access that is not intended for special-purpose or court-ordered use is denied. Modification of a policy is possible yet ineffective in case of existing data. The modified policy only kicks in after the moment of modification, i.e. with future data. Hence, Sealed Analytics ensures better data privacy. *Figure 4* illustrates how Sealed Analytics ensures privacy compliance for Big Data.

Auditing as accompanying organizational measure

Impartial, independent auditing ensures methodical, documented examination of a system. It determines whether quality-reliant activity and concomitant analysis is conducted according to specification and meets the set objectives (audit criteria). A successful audit fulfils specific criteria and conforms to defined requirements. It also implicates two separate procedures that complement each other: A static audit evaluates something according to "handbook". It analyzes whether process documentation meets the set standards specified therein. In contrast, dynamic audits (illustrated in *figure 5*) go much further. The latter consist in continuous system testing.

Conclusion and outlook

Cooperative advanced driver assistance systems based on Car-to-X communication will improve road traffic security considerably. For large-scale application, consumers have to be convinced that these systems improve traffic safety and convenience alike. At the same time, information ethics and legal requirements must also be considered. Hence it is imperative that all data is handled with integrity. Sealed Analytics ensures overall compliance and privacy protection of Big Data from road traffic. It comprehensively safeguards personally identifiable ITS data against abuse, unauthorized access, manipulation and theft. After all, the described technology ensures data privacy observant, compliant analysis, i.e. the sine qua non of political and public acceptance. ■

REFERENCES

(Ahrens et al., 2010) Wissenschaftlicher Beirat beim Bundesminister für Verkehr, Bau und Stadtentwicklung: „Sicherheit zuerst – Möglichkeiten zur Erhöhung der Straßenverkehrssicherheit in Deutschland", in: Zeitschrift für Verkehrssicherheit 56 (2010) 4, pp. 171- 194.

(Albers und Reinhardt, 2010) Albers, M.; Reinhardt, J.: „Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010", in: Zeitschrift für das Juristische Studium (ZJS) 6/2010, pp. 767 – 774.

(BDSG, 2003): Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003.

(Bendel, 2014) Bendel, Oliver: „Fahrerassistenzsysteme aus ethischer Sicht", in: Zeitschrift für Verkehrssicherheit 60 (2014) 2, pp. 108 – 110.

(BfDI, 2012) Bundesbeauftragter für Datenschutz und Informationsfreiheit Peter Schaar: 24. Tätigkeitsbericht 2011 – 2012, published April 24, 2013.

(BMVI, 2012) Bundesministerium für Verkehr, Bau und Stadtentwicklung: IVS-Aktionsplan ‚Straße' – koordinierte Weiterentwicklung bestehender und beschleunigte Einführung neuer intelligenter Verkehrssysteme in Deutschland bis 2020. Berlin (2012).

(DIN, 2008) Deutsches Institut für Normung. DIN V VDE V 0832-500:2008-01: Straßenverkehrs-Signalanlagen – Teil 500: Sicherheitsrelevante Software für Straßenverkehrs-Signalanlagen. Beuth Verlag (Berlin) 2008.

(Douma et al., 2012) Frank Douma, Thomas Garry, and Stephen Simon: "ITS Personal Data Needs: How Much Do We Really Need to Know?", University of Minnesota, Center for Transportation Studies, http://www.its.umn.edu/publications/researchreports , 6/21/2015

(EU, 2008) European Commission: ITS Action Plan / Framework Contract TREN/G4/FV-2008/475/01/ ITS & Personal Data Protection.

(EU, 2010) Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

(Franke et al., 2013) Franke, Kai; Schultz; Holger; Gonter, Mark; Kücükay, Ferit: „Car2Car Sicherheitsfunktionen der nächsten Generation.", in: AAET – 13. Symposium Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel, Braunschweig, February 6-7, 2013, pp. 17 - 29.

(ISO, 2011) Internationale Organisation für Normung. ISO 26262, 2011-04: Straßenfahrzeuge – Funktionale Sicherheit. Beuth Verlag GmbH, Berlin.

(Jäger et al., 2013) Jäger, H., et. al.: "A Novel Set of Measures against Insider Attacks - Sealed Cloud", in: Hühnlein, D., Roßnagel, H. (Eds.): Proceedings of Open Identity Summit 2013, Lecture Notes in Informatics, Volume 223.

(Keil, 2014) Keil, Oliver: „Grundsätze des Datenschutzrechts." https://www2.informatik.hu berlin.de/~keil/docs/Grundsaetze_des_Datenschutzrechts.pdf; 11/6/2014

(Kost et al., 2013) Martin Kost, Raffael Dzikowski, Johann-Christoph Freytag: "PeRA: Individual Privacy Control in Intelligent Transportation Systems", In: Proceedings of the Demonstration Session at the 15th GI-Fachtagung Datenbanksysteme für Business, Technologie und Web (BTW), Magdeburg, Germany, 2013/03

(Köster, 2014) Köster, Frank: „Kooperative Assistenz und Automation in Straßenfahrzeugen – Handlungsfelder/Lösungsansätze/Funktionsbeispiele", In: 15. Symposium Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel, February 12-13, 2014, pp. 87 – 99.

(Rannenberg, 2015) Rannenberg, Kai: „Erhebung und Nutzbarmachung zusätzlicher Daten – Möglichkeiten und Risiken", in: M. Maurer et al. (Eds.): Autonomes Fahren, DOI 10.1007/978-3-662-45854-9_24, (2015), pp. 515-538.

(Rieken et al., 2015) Rieken, Ralf, et al.: „Technische Versiegelung – effektiver Schutz für Inhalte und Metadaten", in: BSI, Tagungsband zum 14. Deutschen IT-Sicherheitskongress 2015, pp. 211-222.

Hubert Jaeger, Dr. sc. techn.
Uniscon GmbH, Munich (DE)
hubert@uniscon.de

Lars Schnieder, Dr.-Ing.
Institute of Transportation Systems,
German Aerospace Center (DLR),
Braunschweig (DE)
lars.schnieder@dlr.de