

BROADEN YOUR LIFE.

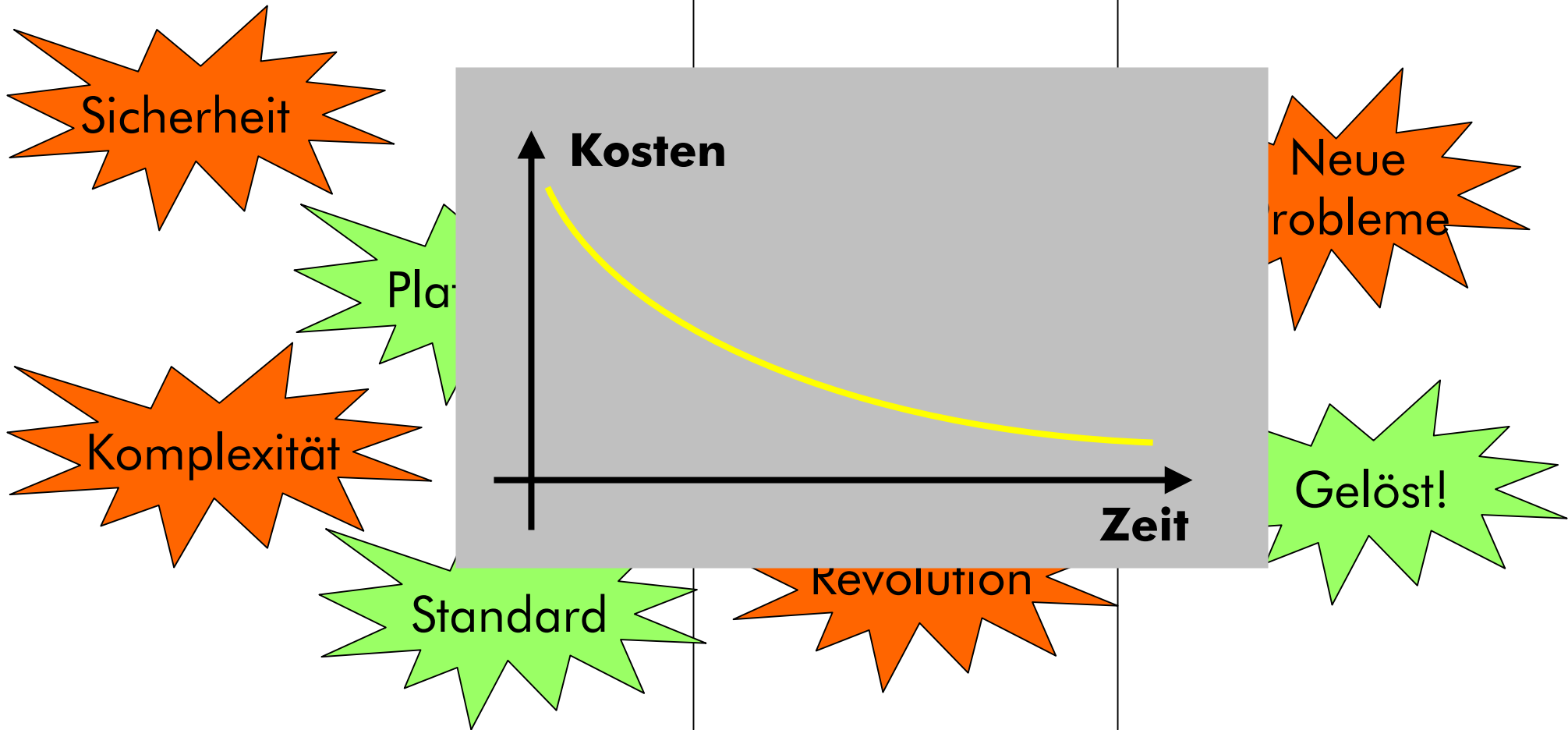


**Offene Systeme ebnen den Weg
in eine sichere Zukunft**



Assoziationen

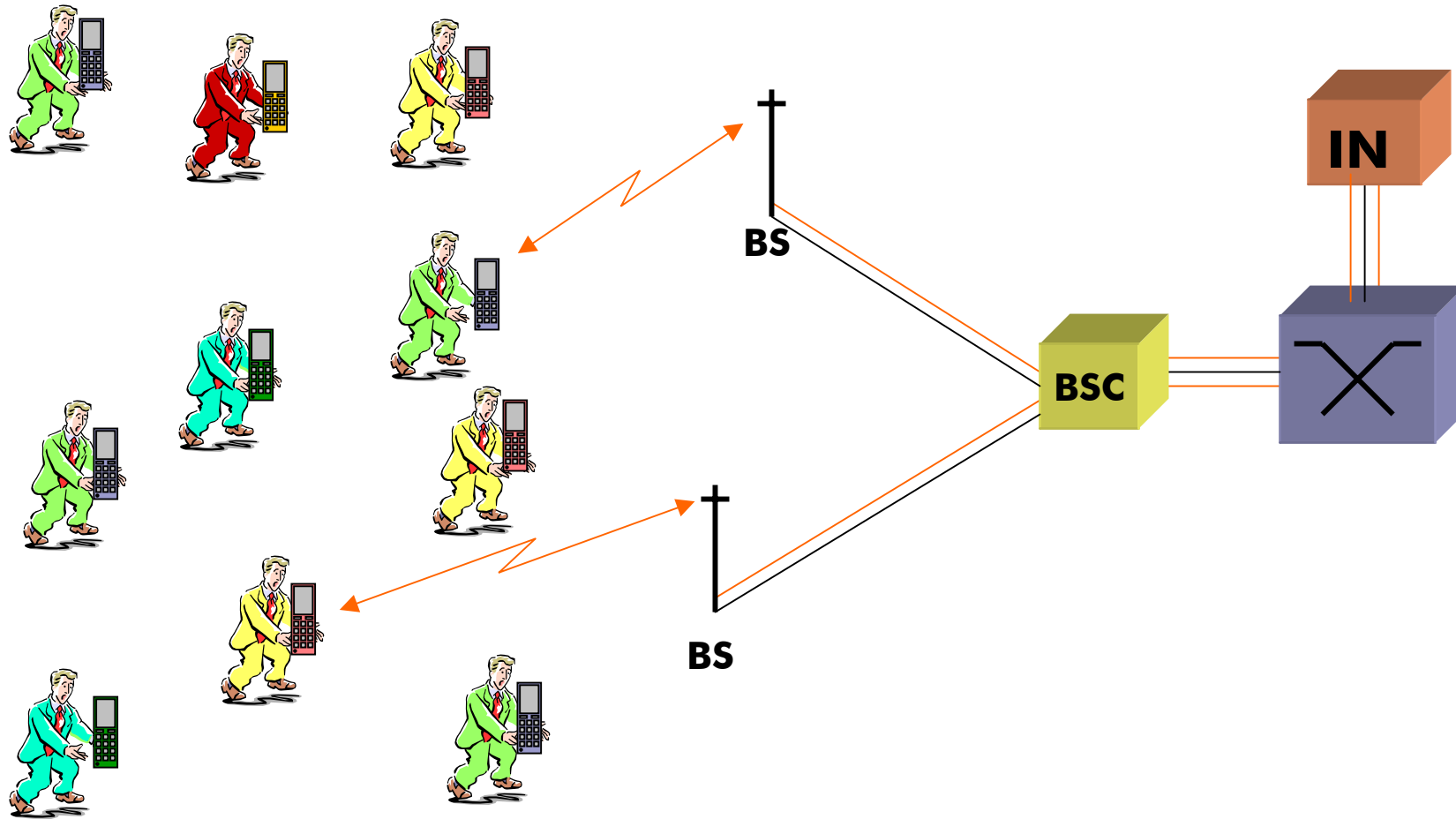
Offene Systeme ebnet den Weg in eine sichere Zukunft



Agenda

- > Offene Systeme – ein Muss in der Telekommunikation
- > Offene Systeme – eine Chance für Telematik-Systeme
- > Offene Systeme – eine Herausforderung an die Realisierung

Ein Muss in der Telekommunikation



Ein Muss in der Telekommunikation - Standardisierung

> Weltweit

- ITU (International Telecommunication Union)
- ISO (International Organisation for Standardisation)
- IEC (International Engineering Consortium)

> Europaweit

- ETSI (European Telecommunications Standards Institute)
- CEN (Comité Européen de Normalisation)
- CENELEC (Comité Européen de Normalisation Electrotechnique)

> Deutschlandweit

- DIN (Deutsches Institute für Normung)
- DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik)

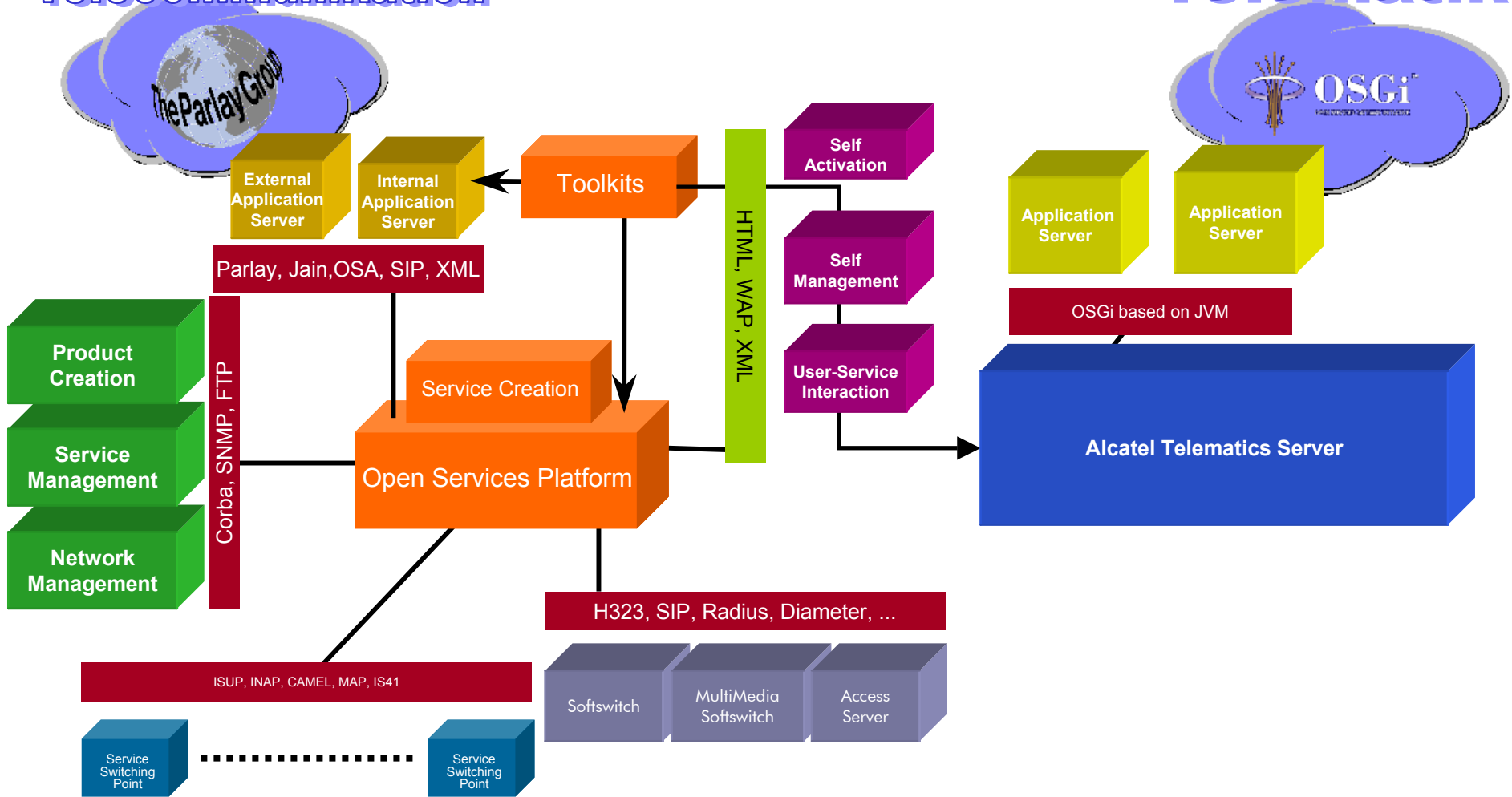
IEEE (Institute of Electrical & Electronical Engineering)

IETF (Internet Engineering Task Force)

Ein Muss in der Telekommunikation - Realisierung

Telekommunikation

Telematik



Agenda

- > Offene Systeme – ein Muss in der Telekommunikation
- > Offene Systeme – eine Chance für Telematik-Systeme
- > Offene Systeme – eine Herausforderung an die Realisierung

Markt für Telematik-Dienste

> Politik, Regulierung

- Elektronische Mautsysteme
 - Stau-Management
 - Verkehrsmessungen
- Elektronischer Fahrtenschreiber
- Black box

> Sich verbreitende Logistiklösungen

- Supply Chain Management
- Enterprise Resource Management
- RFID Technik

> Intelligenterer, mobile Endgeräte

- Smartphone, PDA
 - Rechenleistung, Display
 - Kommunikation, Positionierung

**Telematik
Lösungen**



> Fragmentierter Markt

- Verschiedenste Lösungen
- Intermodalität
- ...

> Sich entwickelnde Fahrzeugtechnik

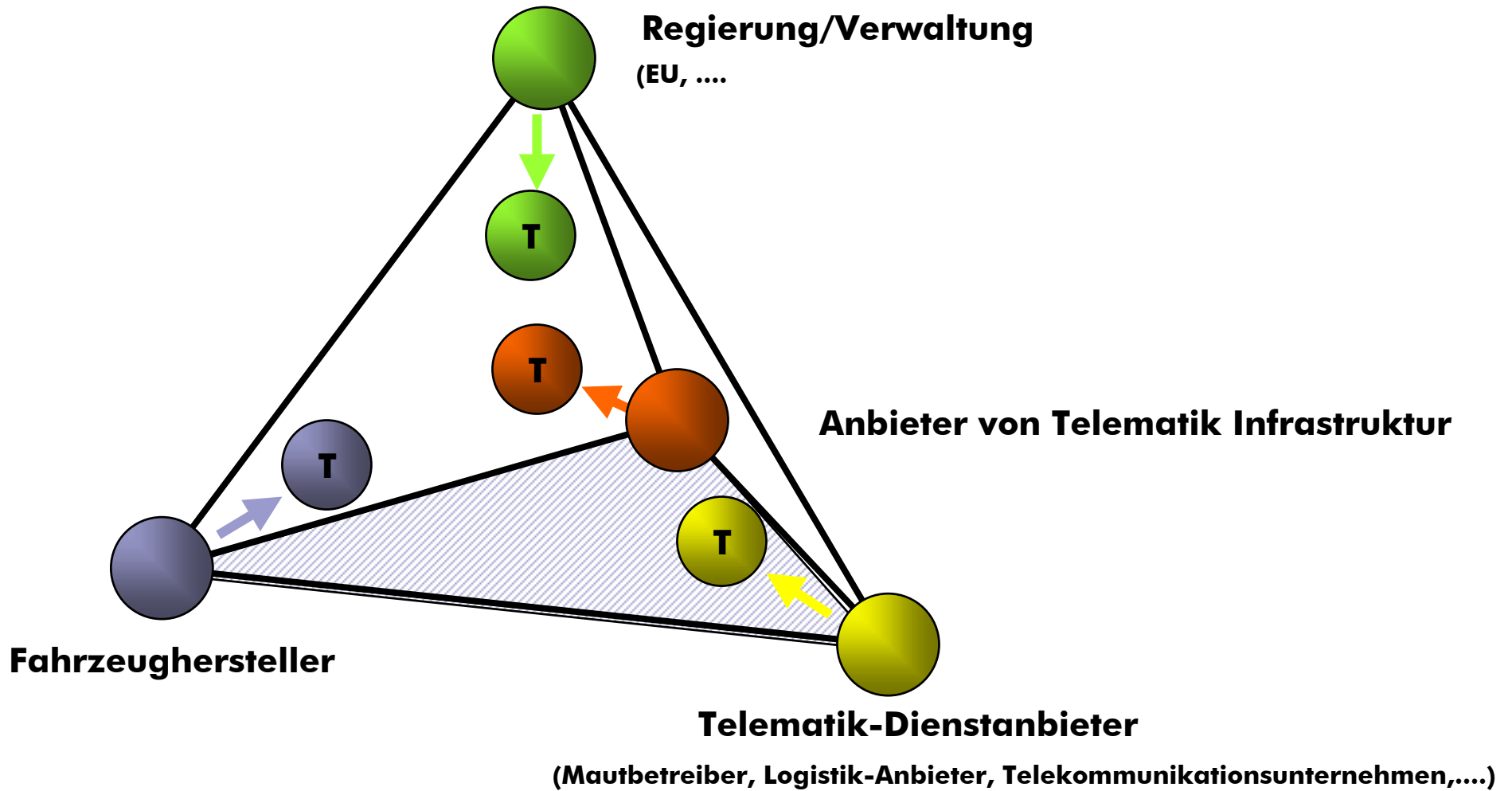
(Zunahme von Elektronik & Software)

- Datenbusse in Fahrzeugen erlauben Daten- und Steuerungszugriff
- SW-Erweiterung für "embedded systems"
- Diagnose-Systeme für "embedded systems"
- Integration von Unterhaltungssystemen (bedeutender im Markt für PKWs)

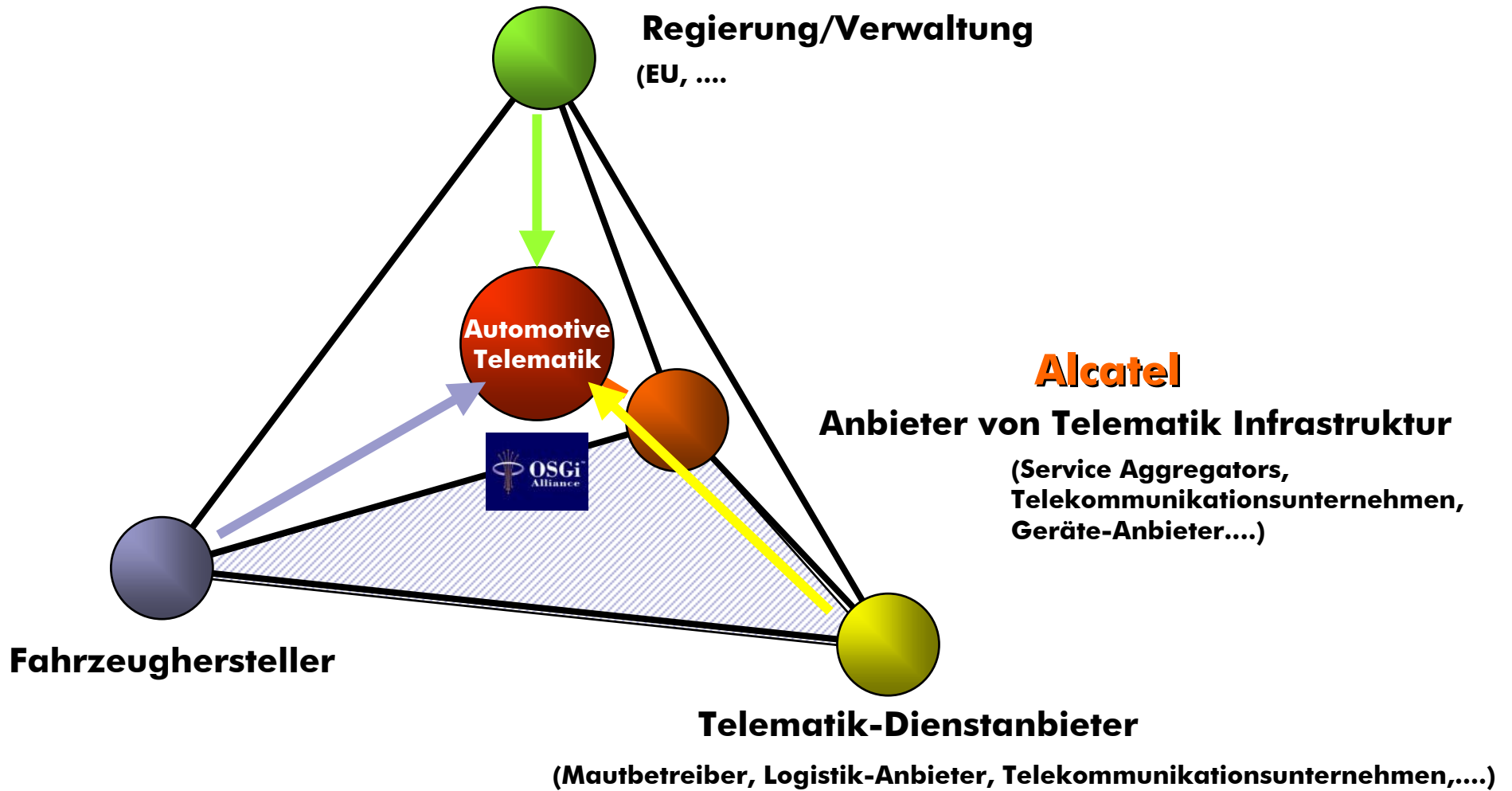
> Bedenken von Herstellern/Kunden

- Gewährleistung der Fahrzeugintegrität
 - Garantie eines "sicheren" Zugangs
 - Garantie für sicheren Betrieb
 - Schutz gegen Missbrauch
- Divergierende Lebenszyklen für IT-Geräte & Fahrzeuge

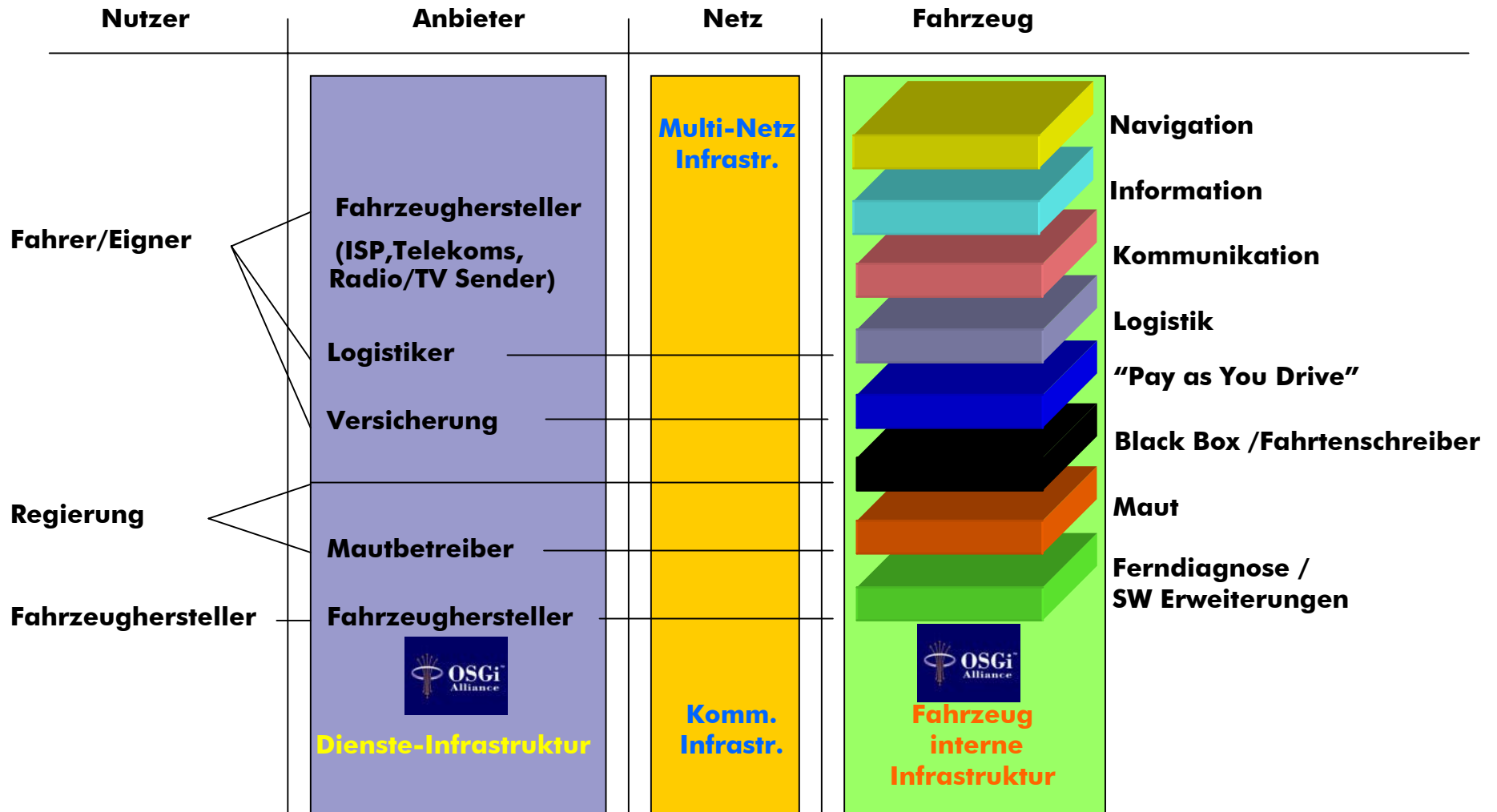
Telematik - heute



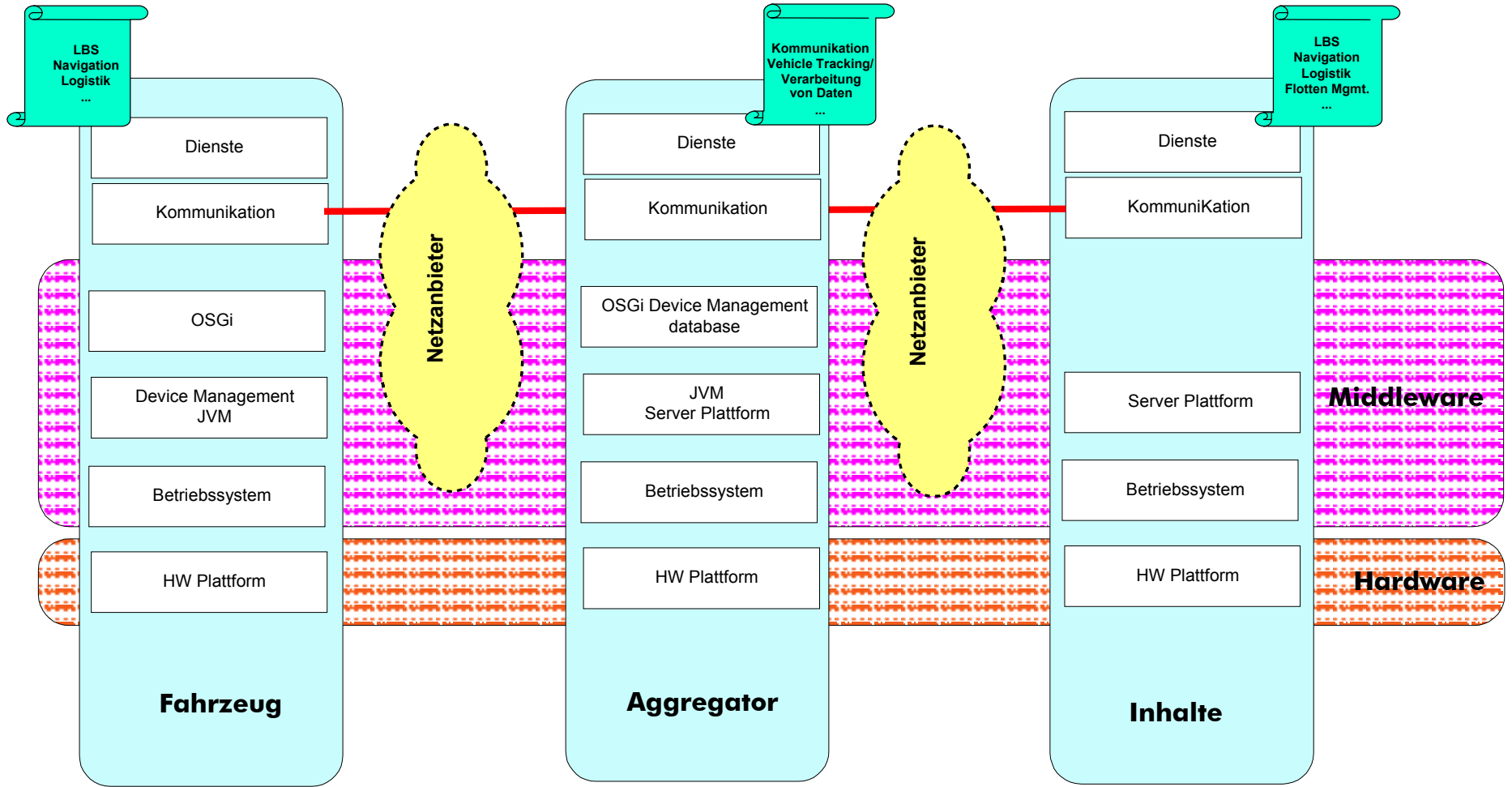
Telematik - morgen



Konzept eines Telematik-Systems



Allgemeine Architektur



Agenda

- > Offene Systeme – ein Muss in der Telekommunikation
- > Offene Systeme – eine Chance für Telematik-Systeme
- > Offene Systeme – eine Herausforderung an die Realisierung

Eine Herausforderung an die Realisierung

> Sicherheit

- Zukunftssichere Systeme
- Datensicherheit, Integrität von Algorithmen und Verfahren

> Verfügbarkeit

- Technische Verfügbarkeit von Systemen
- Mobile Anwendung -> örtliche Verfügbarkeit -> Multi-Netz-Systeme
- Diensteverfügbarkeit auf verschiedenen Geräten

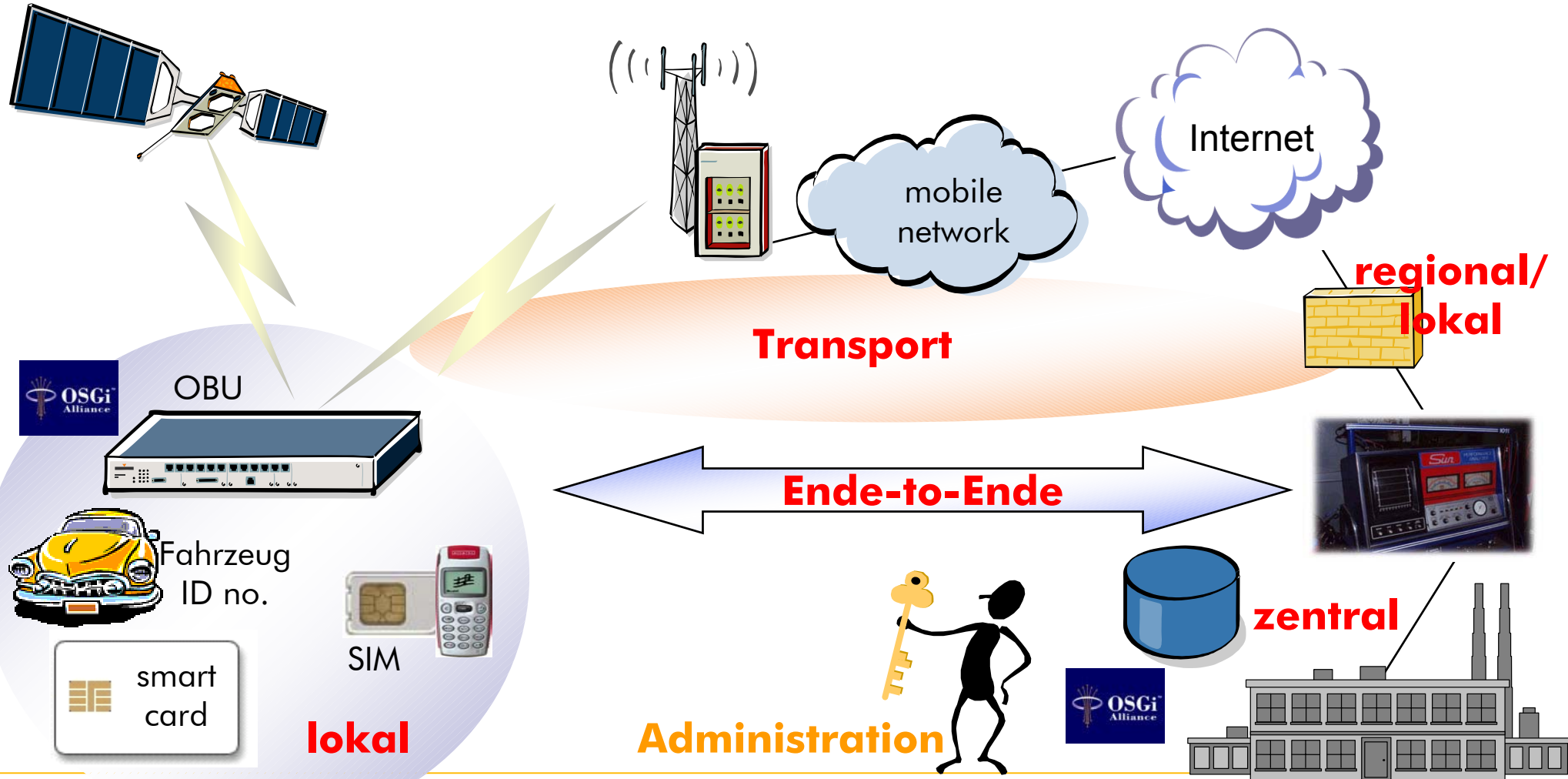
> Integration

- Verfügbares Einbauvolumen in Fahrzeugen
- Funktionale Integration verschiedenster Anwendungen

> Kosten

- Infrastrukturkosten
- Kosten für Dienste

Sicherheitsbereiche - System Konfiguration



Bedrohungen

- > "Reverse Engineering"
Analyse der Architektur und des Speichers,
Fälschungen (Identität, Maut, Überwachung/Position, ...)
 - in der OBU
 - in Fahrzeugdiagnosesystemen
- > Abhören
- > Manipulation von Meldungen und Speicherinhalten
- > manipulierte Downloads ("tuning")
- > Sabotage (falsche Schlüssel, Zugriff auf Fahrzeugbus, ...)

Anforderung an Sicherheitsfunktionen

> Authentisierung

- gegenseitige Authentisierung
- Identität des Fahrzeugs (Fahrzeugnummer, Version) und verantwortlicher Service Organisationen
- Beglaubigungen (SIM, shared key, certificate, PIN, equipment serial no., ...)

> Vertraulichkeit

- lokaler Speicher (Daten, Schlüssel)
- sichere Übertragung (individuell und multicast)

> Sichere Inhalte

- signierte Daten (Integrität und Verifizierung der Herkunft)
- sichere Multicast-Verteilung

> Sicheres Schlüssel-Management

Sicherheitsfunktionen im Fahrzeug-Equipment

- > Authentisierung
- > Verschlüsselung
- > Signaturen
- > Schlüssel Management
- > Sichere Speicher für Schlüssel, Algorithmen und Daten

Zusammenfassung

> Es gibt hinreichende Erfahrung mit offenen Systemen.

➔ „Erfahrungstransfer“

> Verschiedenste Teleematik-Anwendungen benötigen eine gemeinsame Plattform.

➔ Offene Systeme mit Nutzung gemeinsamer Ressourcen

> Die Schaffung von Akzeptanz hat oberste Priorität.

➔ Sicherheit, Kosten, Verfügbarkeit, ...

www.alcatel.com