



**i2010 –  
Intelligent Car**

# Mastering the Security Gap

	Smart Autonomous Decision Taking	Clean	Safe & Secure
Reliability	Next Generation Sensor Development		
Co-operative Systems	Next Generation Assistance Systems		
Networked Systems			
<b>Assessment &amp; Demonstration Projects</b>			

**Protection of  
Digitally stored Data  
& Telematics**

**Avoidance of  
direct Access of eComponent  
& Systems (wireless &  
wire-connected)**

**Protecting  
Networked Vehicles  
from remote Access**

Technology itself cannot guarantee security, but security without the support of technology is impossible. It provides information about threats, helps to build effective protection against them and, if necessary, enables to neutralize them. In other words: technology is a key “force enabler” for a more secure Europe.

An initial set of actions, identified for the technological part was compiled and edited:

**1. Protection against mobile remote access on networked vehicles**

- e.g. On vehicles with mobile communication and/or internet connections
- e.g. On applications of V2V and/or V2I communication

**2. Protection of motor vehicles (full electronic system and components) against manipulation of**

- external wireless remote data-transfer
- external wire-connected access (diagnostics-points, user-ports, etc)
- structural manipulation of the vehicles' electronic on-board system

**3. Protection of electronic motor vehicle components against**

- mal-function of non-certified components
- late implementation of non-certified software, e.g. Trojans, Viruses, Spy-Ware,..

**4. Protection of digital data stored in the motor vehicle against unauthorised access and manipulation of:**

- o software know-how of electronic vehicle components,
- o personal operational and localisation information,
- o commercial digital media (e.g. CD:s/DVD:s for digital maps, audio/video),
- o business and personal data (mobile office),
- o wireless payments in motor vehicles (billing concepts, e-payments, etc.).

**5. Protection of motor vehicles and fleets by securing telematics and co-operative system applications:**

- fleet management (e.g. for disaster management, rescue services, Fire brigades, police, military) manipulation in mission control of specified fleets,
- mobile traffic data capture via on-board sensors, based on XFCD (Extended Floating Car Data) technologies, in order to avoid manipulation of traffic flows,
- navigation services (e.g. for off-board navigation or hybrid navigation) to avoid manipulation of dynamically created routes within an infrastructure,
- remote diagnostics and remote repair to avoid misleading vehicle diagnostics and recommendations,
- unauthorised software download to prevent the implementation of uncertified software.

# i2010 – Convergence of automotive ICT

	<b>Smart Autonomous Decision Taking</b>	<b>Safe &amp; Secure</b>	<b>Clean</b>
<b>Reliability</b>	<p><b>Next Generation</b> Intelligent braking &amp; Driving</p>	<p><b>Sensor Development</b> Independent local power supply</p>	<p>Enhanced ACC Systems for Trucks</p>
<b>Co-operative Systems</b>	<p><b>Next Generation Assistance Systems (Driver Monitoring)</b></p>	<p>Optical Communication  Protected connections (Automotive Fire walls)</p>	<p>Environmentally influenced Powertrain Control</p>
<b>Networked Systems</b>		<p>Car-to-Car Communication</p>	<p>Navigation- assisted Powertrain Control</p>
<b>Assessment &amp; Demonstration Projects</b>			



# Target Concept: „Mobile, Accident-free & Secure Vehicle of the Future”

Discipline	Technology	Needs				Applications
		<b>Increasing Functionality</b>	<b>Higher Complexity</b>	<b>Competitiveness of embedded Software “Managing the Productivity Gap”</b>	<b>Networking &amp; Distributed Systems</b>	
<b>eSecurity</b>	<b>Authorization Identification Technologies</b>	<b>Info Anonymity &amp; Authentication Processes</b>	<b>Certified No. of Data Sets</b>	<b>Accessible Inter-Layers, Open Source Systems</b>	<b>Abuse of external Networks &amp; Signals</b>	<b>Anti-Jamming</b>
	↓	<b>Holistic &amp; Domain specific Risk Analysis</b>	<b>Hyper-reactive Encryption Technologies</b>	<b>End-to-end Source Transmission Channels</b>	<b>Data Encyption Frequency hopping Broad-Band Techn.</b>	<b>Data Privacy Assurance</b>
	↓	<b>Protection Rules &amp; Standards</b>	<b>Cryptographic Routers</b>	<b>Anti-Spam Technologies</b>	<b>Resident Data Security Technologies</b>	<b>Automotive Fire Wall &amp; Virus Protection</b>
	↓		<b>Data security</b>		<b>Secure Data Communication</b>	
	↓	<b>secure, highly integrated Microsystems</b>	<b>Micro-systems actuator alternatives – Integration in vehicle architecture</b>	<b>Robust &amp; continuous Connectivity coupled with logical diversity (multi-protocol service flexible, self-adapting routing, automatic recovery procedures</b>	<b>Authorisation Mechanisms &amp; Access Control</b>	<b>Secure On-board Unit</b>



# Target Concept: „Mobile, Accident-free & Secure Vehicle of the Future”

Discipline	Technology	Needs				Applications
		<b>Increasing Functionality</b>	<b>Higher Complexity</b>	<b>Competitiveness of embedded Software “Managing the Productivity Gap”</b>	<b>Networking &amp; Distributed Systems</b>	
<b>eSecurity</b>	<b>Vehicle Drive &amp; Usage Control</b>	Detecting/ Correcting codes	<b>High Security Micro Controllers</b>	Quality of Signal for priority services	<b>Authorization of Ad-hoc Networks</b>	
	chemical surface technologies	Biometrics for user authentication			<b>Inter-Layer Access</b>	
	chemical active materials					<b>Gas-, bio-, explosives-, nuclear Sensors</b>
	<b>Billing Systems</b>					<b>Road pricing systems</b>
	<b>Contract Management</b>					
	<b>Warranty &amp; Documen- tation</b>					



# Target Concept: „Mobile, Accident-free & Secure Vehicle of the Future”

Discipline	Technology	Needs				Applications
		<b>Increasing Functionality</b>	<b>Higher Complexity</b>	<b>Competitiveness of embedded Software “Managing the Productivity Gap”</b>	<b>Networking &amp; Distributed Systems</b>	
<b>eSecurity</b>	<b>Legal &amp; Liability Topics</b>		<b>Standards/ Legislation</b>	<b>Security labelling against product piracy</b>		

# Proposed draft Terms of Reference of a Working Group: “eSecurity” Technologies

## What should the group investigate?

Investigate IC Technologies, which cover the vulnerability to Road Transport introduced by the abuse of networked and co-operative systems. It has to complement the functional (threat treatment) and administrative (legislation) wings with the identification of the requisite technology a key “force enabler”. Therefore a joint effort of industry, infrastructure operators, public authorities and users is highly important.

- ✎ **Protection against mobile remote access on networked vehicles**
- ✎ **Protection the full electronic system and its components against manipulation (e.g. wired & tele- data transfer)**
- ✎ **Protection of electronic motor vehicle components against e-assaults (e.g. viruses, trojans, spy-ware, etc.)**
- ✎ **Protection of digital data stored in the motor vehicle against unauthorised access and manipulation**
- ✎ **Protection of motor vehicles and fleets by securing telematics and co-operative system applications**

## Who should be in the group?

About 10 – 15 persons representing all stakeholders Automotive Manufacturers and Suppliers, Telecom Operators and Service Providers, Authorities and Road Operators, Research Establishments and Academia