**Project no.:** **IST-FP6-STREP-26979**

**Project full title:** **Highly dependable ip-based networks and services**

**Project Acronym:** **HIDENETS**

# Deliverable no.: D8.3

# Title of the deliverable: Publishable Activity report

| | |
|---|---|
| **Contractual Date of Delivery to the CEC:** | 15 May 2009 |
| **Actual Date of Delivery to the CEC:** | 29 May 2009 |
| **Project coordinator organisation name:** | P01 AAU, Aalborg University |
| **Project coordinator name:** | Hans Peter Schwefel |
| **Participant(s):** | All partners |
| **Period cover:** | **From: 1 Jan 2006 to: 31 March 2009** |
| **Nature:** | Report |
| **Version:** | Ver. 1 |
| **Total number of pages:** | 30 |
| **Start date of project:** | 1st Jan. 2006 **Duration:** 39 months |

| **Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)** | | |
|---|---|---|
| **Dissemination Level** | | |
| **PU** | Public | **X** |
| **PP** | Restricted to other programme participants (including the Commission Services) | |
| **RE** | Restricted to a group specified by the consortium (including the Commission Services) | |

## HIDENETS

### Highly DEpendable ip-based NETworks and Services.

HIDENETS is a Specific Targeted Research Project (STREP) in the European 6th Framework Program running in the period from January 2006 to March 2009. It developed and analyzed end-to-end resilience solutions for distributed applications and mobility-aware services in car-to-car communication scenarios with infrastructure service support. Thereby, the concept of resilience extends the classical notion of fault tolerance, usually applied to recover system functions in spite of operational faults, to some level of adaptability, so as to be able to cope with system evolution and unanticipated conditions. Main results of HIDENETS are: (1) Design and evaluation of a run-time resilience support via a set of middleware and communication level functions; (2) A holistic evaluation framework for quantitative analysis of dependability properties of HIDENETS-like applications in highly mobile settings; (3) Design methodologies and tool support for the development and testing of resilient applications on top of the HIDENETS middleware; (4) Prototype implementation and evaluation acting as proof-of-concept of key aspects of the HIDENETS solutions; (5) Dissemination material including a detailed tutorial of over 900 slides. The HIDENETS solutions contribute to a user perception of trustworthiness of future wireless services, as this perception is strongly impacted by availability and resilience aspects. Such perception is critical for the technical and business success of these services.

The solution development and analysis required a holistic approach combining aspects of communications, middleware, service deployment and access. Hence the research work combined forces from the engineering community and from leading research teams on resilient distributed systems: Universities of Aalborg (DK), Budapest (HU), Lisbon (PT), Florence (IT); Carmeq (GER), Fujitsu Siemens Computers (GER), LAAS-CNRS (FR), Telenor (NO), Twente Institute WMC (NL).

### Partner logos

FUJITSU COMPUTERS SIEMENS

CNRS LAAS

WMC

MŰEGYETEM 1782

carmeq

FACULDADE DE CIÊNCIAS UNIVERSIDADE DE LISBOA

AALBORG UNIVERSITY DENMARK

STVDIORVM · VNIVERSITAS · FLORENTINA

telenor

# Table of Contents

# Publishable executive summary

## 1 Background

HIDENETS addresses the provision of available and resilient distributed applications and mobile services with critical requirements on highly dynamic and possibly unreliable open communication infrastructures. Such ubiquitous infrastructures consist of networking scenarios made of ad-hoc/wireless multi-hop domains as well as infrastructure network domains. The concept of resilience thereby extends the classical notion of fault tolerance usually applied to recover system functions in spite of operational faults, to some level of adaptability, so as to be able to cope with system evolution and unanticipated conditions. The technical solutions in HIDENETS account for environments with the following characteristics:

- The presence of wireless links is a cause for inherent unreliability of communication.
- The use of commercial off the shelf (COTS), standard compliant systems and components, integration of legacy subsystems as well as the use of development tools is a must.
- The services must be scalable w.r.t. number of users or traffic flows, costs, system infrastructures.
- Highly dynamic network topologies are an underlying property of the deployment infrastructure.

Resilience and availability of services deployed either in an ad-hoc domain or on dedicated servers in the infrastructure network have to be taken into account on a system design level, since the components are inherently unreliable. This problem is aggravated by the coexistence of accidental and malicious faults (attacks and intrusions).

## 2 Project Objectives

The objective of HIDENETS is to develop innovative technological solutions to allow deployment of services with high dependability requirements using components and communication links that are inherently unreliable. Current state-of-the-art solutions are limited to individual components and functionalities while HIDENETS follows a holistic end-to-end system approach, jointly considering communication aspects as well as service and middleware functionalities. The scientific and technological objectives are:

- Provide architectural and design solutions concerning both network/protocol elements and technology components and their ensemble as ‘middleware’, required for the deployment of highly available and resilient mobility-aware services.
- Identify development tools and mechanisms like design patterns and testing methodologies to assist the implementation of said service qualities.
- Develop methodologies for the quantitative evaluation and analysis of the achieved QoS of applications and services.
- Provide an implementation of the relevant parts of the design solutions to constitute a proof of concept prototype in the automotive application domain covering both ad-hoc car-to-car and server based (infrastructure) scenarios.
- Perform an assessment of the dependability and QoS provided by the solutions developed in HIDENETS through the evaluation of the selected scenarios both at model resolution level and at the experimentation on the proof-of-concept experimental test beds.

**The HIDENETS results clearly show that solutions for new distributed applications with critical requirements on open communication infrastructures can be designed, implemented, and evaluated in a holistic fashion.**

In addition, the creation of awareness for high availability and resilience as foundational service qualities and the dissemination of methods and tools for the development and deployment of highly available, resilient services have been focal project objectives.

# 3 Partners in the consortium

| **Participant name** | **Participant short name** | **Country** |
|---|---|---|
| Aalborg University (Coordinator) | AAU | Denmark |
| Budapest University of Technology and Economics | BME | Hungary |
| Carmeq GmbH | Carmeq | Germany |
| Fujitsu Siemens Computers | FSC | Germany |
| Centre National de la Recherche Scientifique | LAAS-CNRS | France |
| Telenor | Telenor | Norway |
| Fundação da Faculdade de Ciências da Universidade de Lisboa | FCUL | Portugal |
| Twente Institute for Wireless and Mobile Communications B.V. | WMC | The Netherlands |
| Universitá degli studi di Firenze | UNIFI | Italy |

# 4 Results of the project

## 4.1 Scope and use case scenarios

HIDENETS addresses the provisioning of available and resilient distributed applications and mobile services in highly dynamic environments characterised by unreliable communications and components. The investigations include networking scenarios consisting of *ad hoc*/wireless (multi-hop) domains as well as infrastructure network domains. Applications and use case scenarios from the automotive domain [3], based on car-to-car communications with additional infrastructure support, have been used in an exemplary manner to identify the key challenges, threats, and resilience requirements that are relevant in the context of the project.

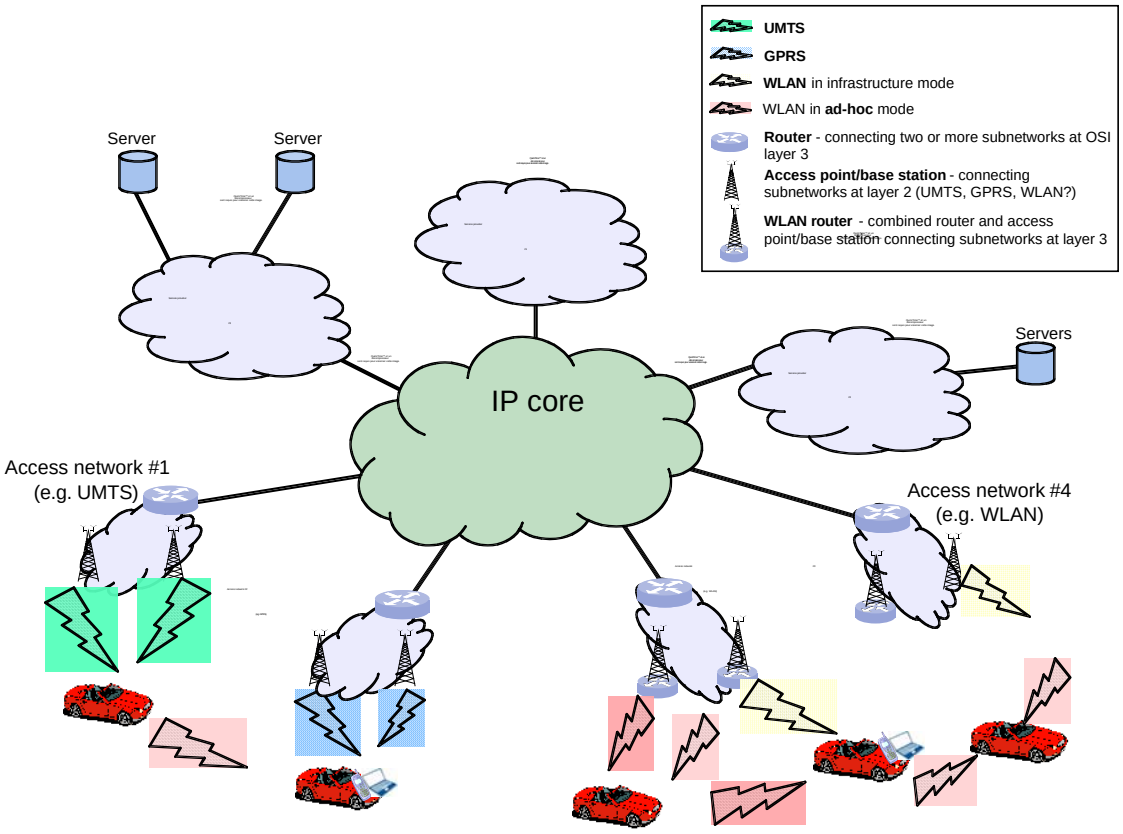


**Figure 1: HIDENETS network architecture – infrastructure and ad hoc domains**

The HIDENETS **communication scenario** is illustrated in Figure 1. We distinguish two different domains: 1) the ad hoc domain in which service access and service deployment are performed in a wireless setting, and 2) the infrastructure domain that consists of a back-bone IP network connecting both service providers as well as service clients. Parts of the ad hoc domain may be connected to the infrastructure domain via cellular access (GPRS/UMTS) or via WLAN Road Side Units (RSUs). As illustrated in Figure 1, mobile nodes communicate with other mobile nodes directly or via the infrastructure domain. In the HIDENETS scenarios, these nodes will typically be cars, but they may also be car-external devices. Mobile nodes may also communicate with nodes in the infrastructure domain.

A HIDENETS **use case** is a set consisting of (one or more) applications, the actors and roles involved, and the identification of the affected dependability domains. The identified applications for a use case are assumed to occur in a certain context where these applications typically appear together and interact with each other. The actors and their roles represent the glue of the use case and are important for the interaction between the applications. Within HIDENETS, 17 applications were identified and 6 use case scenarios were formed out of them [3]. The criteria for choosing these use cases and applications have been derived from supposed user needs and new functionalities obviously useful in future traffic scenarios. Beyond that,

HIDENETS use cases were carefully adjusted in accordance to current discussions and trends in the automotive domain and the Car2Car Communication Consortium [13].
Large part of the research work in HIDENETS was motivated by three main use cases which impose complementary challenges and functionalities:

- Infotainment: Depending on the available user-interaction modalities, the applications in this use case may be mainly accessed by passengers. Employees while travelling may want access their company's intranet to get access to or upload important documents, update their calendars, check email, meet some deadline, etc. While travelling, they may take part in a teleconference. Other passengers may want to play online games, watch TV or a video, collect tourist information about the scenery passing by, or shop products on the web. The challenge in this use-case is to meet the user-perceived application quality expectations despite the high mobility, multitude of different devices participating, and wide diversity in the applications requested.
- Platooning: This application is a step towards automated driving, in which the leading car is driven by a human and sends control information to the following cars; the followers immediately have to process the control data and act accordingly, while they try to follow the leading car as closely as possible. A close distance facilitates saving energy consumption by driving in the slipstream of the car in front. Therefore, all subsequent cars of a platoon are not controlled by humans. For this application, timeliness of data communication and message processing is essential to assure safety.
- Car accident: This use-case evolves around a scene with an accident on a road, involving cars and other road users. The use case covers what happens after the accident, but also involves some issues directly before and during the accident. Directly before the accident, the distributed black-box functions of the cars in the area collect time-stamped information. This information is backed up to other cars as they pass, as well as to fixed-network servers whenever access to the fixed infrastructure is available. The higher the percentage of cars that is equipped with the black-box functionality, the lower is the risk of losing data. Right after the accident, many people may try to call the emergency services, call home, and send text and multimedia messages, at least in motorways with high traffic density. This may cause congestion in the radio access network, both in WLAN-type technologies and in mobile networks. It is a challenge for the networks to be able to prioritise between the requested services. Some time after the accident, an ambulance is approaching and the cars along the road are notified either directly through the ad-hoc network or via the infrastructure network and road-side access points that broadcast the message to the cars along the particular road segment. The alarm centre personnel may already at this stage know the names of the persons involved in the accident, and even pictures may have been transferred from the accident scene. Essential data on the injured, along with possible pictures of the crash scene, may be transferred to the ambulance while on its way. Arriving at the place in question, there may be a need to communicate with medical expertise at the local or a central hospital by use of voice, video and data transmission (multi-media application). There may also be a need for group communication with other emergency teams at the site. Heading back to the hospital with the injured there will be a need to transmit information on the positioning of the ambulance to communicate that it is approaching the hospital and at the same time maintain the multimedia connection with the medical expertise. Afterwards, the cause of the accident can be analyzed by investigating data collected by the distributed black box application.

The platooning use case imposes primarily timeliness requirements and relies mainly on car-to-car communication – though enhancements, e.g. for consensus achievement [16], can result in presence of infrastructure connectivity. The infotainment use case addresses a classical scenario in which online content can be accessed via car-to-car and car-to-infrastructure communication. This imposes real-time and QoS needs, but also trustworthiness requirements. Applications in the car accident use case contribute to avoiding and alleviating fatalities and accident reconstruction possibilities via the distributed black box. The car accident use case describes again a scenario which is based on both car-to-car and car-to-infrastructure communication, but here the requirements impose a stronger focus on service differentiation and resilience mechanisms, which need to be balanced based on the current phase of the use case. Dependability requirements in this use case scenario also concern the integrity and the availability of the data collected, this is in particular the case of the distributed black-box application.

## 4.2 Overview of the main results

Driven by the challenges and requirements of the use-cases, the HIDENETS project has developed appropriate **run-time resilience support** via fault-prevention and fault-tolerance mechanisms at the middleware and communication layers. Furthermore, the project adopted appropriate architectural constructs, as well as methodologies to support the design, development, evaluation, and testing of dependable solutions using such mechanisms. This section contains an overview of the key results; for an overview on individual functions, see Reference [22]. Detailed descriptions and derivations are presented in the HIDENETS deliverables [4,5,6,16,17,18,19,20,21,24,61].

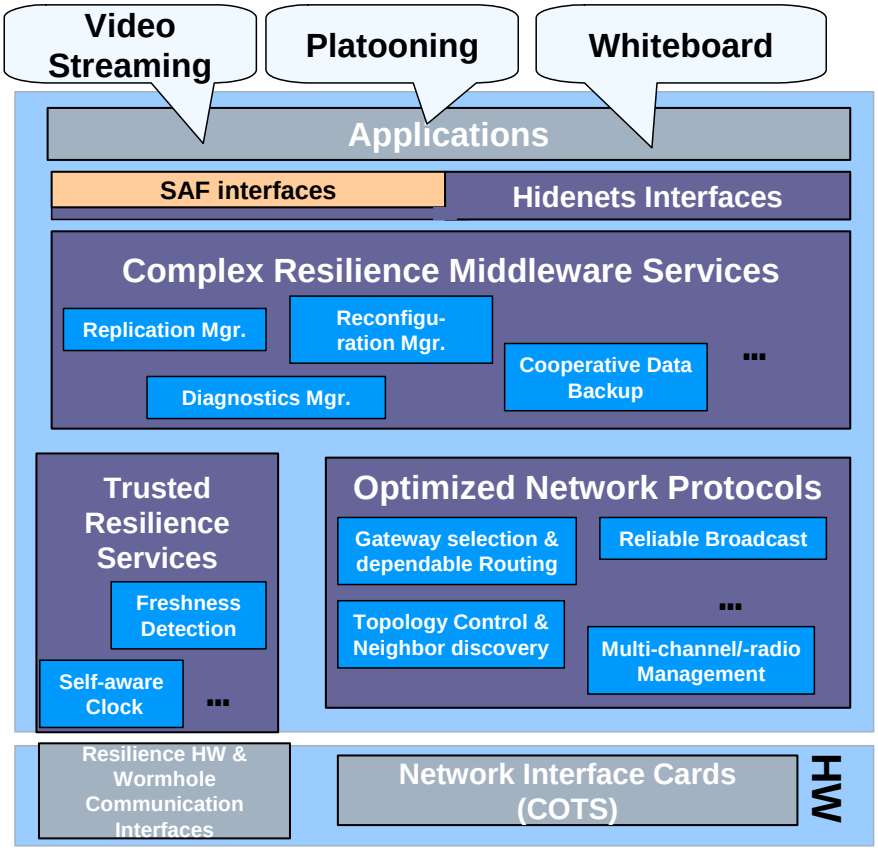


**Figure 2: HIDENETS dependability architecture including a subset of the functionalities developed in the project; for a complete list see References [22,2,4,5]. The dark shaded architecture parts mark the technical scope of HIDENETS.**

Figure 2 shows the architecture and a subset of the dependability related functions that have been developed in HIDENETS. The main elements of this architecture are:

- *Middleware dependability services*: These functions enable protection and fault-tolerance for application programs and their data. Functionalities include data replication and efficient access to distributed fault-tolerant storage, error detection and fault diagnosis, as well as recovery actions for different fault scenarios. See [2,4,16,17] for more details. Some of these functionalities need to be accessed by the applications. Although standardised interfaces [12] are utilised as far as possible, specific functions addressing the dynamicity of the ad-hoc networking scenario require the specification of additional interfaces [4,8,61].
- *Enhanced communication protocols*: The geographic mobility of the vehicular nodes leads to rapidly changing ad-hoc network topologies, fluctuating communication link properties, and changing points of attachment to the infrastructure domain. Resilient communication in HIDENETS is achieved via extensions of the Link and Network Layer functionality, including management of multiple interfaces, robust routing and broadcasting schemes, and traffic differentiation. See [5,18] for details.
- *Architectural hybridization*: As certain critical functionalities should remain unaffected by the most frequent fault cases, HIDENETS employs the concept of architectural hybridization, which architecturally separates these functionalities; see the lower left of Figure 2. The architectural separation is also applied to the communication functions and interfaces for these distributed dependability services [4,16,17,19].

An overview of the middleware and communication level services, their design and lessons learned in HIDENETS can be found in Chapter 3 of Reference [22], details in References [4,5,16,17,18,19].

The feasibility and the practical relevance of the HIDENETS run-time dependability solutions have been validated in three **proof-of-concept test beds [24,20]**. These laboratory implementations consist of the integration of the essential outcomes of the HIDENETS analysis and development work in order to focus on essential functionalities and to show the benefits of a flexible and modular HIDENETS architecture. The three test-beds are

- **Platooning test-bed**
  A platooning prototype application that is used as a proof-of-concept for the ability to detect and react to timing faults, to assure safety and to handle certain malicious intrusions. Figure 3 shows its basic setup.
- **Distributed Black-Box test-bed**
  A distributed black-box application showing a car-to-car cooperative and secure backup scheme for critical data, and a resilient store and retrieval system. Figure 4 shows a picture of the actual operation of the testbed.
- **Resilient Communication test-bed**
  Selected optimised communication protocols for ad-hoc car-to-car (c2c) networks and their impact on higher network layers.

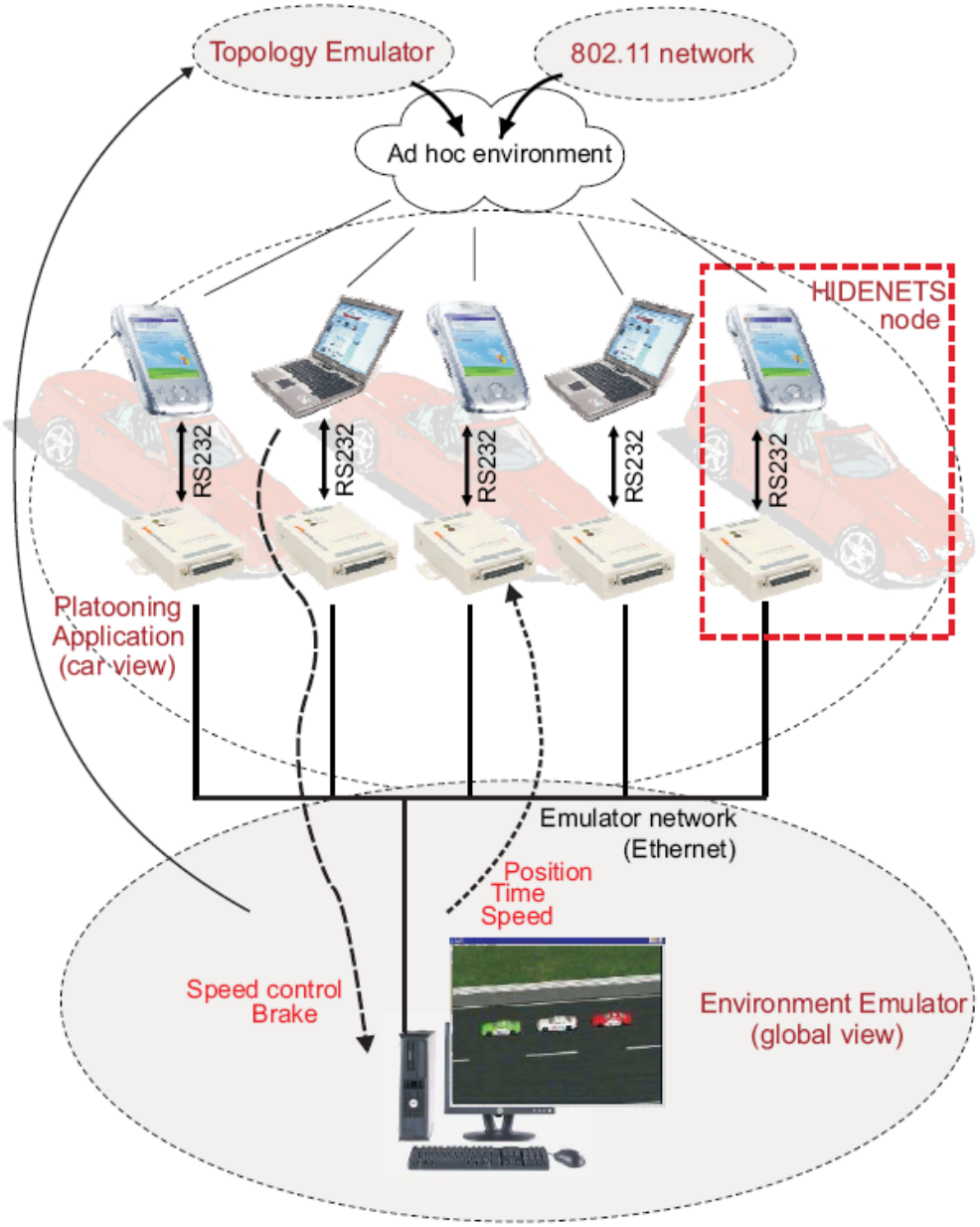


**Figure 3: The platooning testbed schematic setup; mobility is emulated in the Environment Emulator (bottom) and mapped to dynamic communication properties via a topology emulator (upper left)**

There is also a fourth testbed, called **application development testbed**, whose scope however is not the run-time dependability support. Hence it is described further below

Reproducible experiments for mobile scenarios have been realised using emulated dynamic multi-hop communication topologies and via scaling down mobility and communication properties to lab-size setups, see Reference [20,24]

**Figure 4: Scaling down mobility and wireless communication to lab-size in the distributed black-box testbed**

In order to analyse the dependability and QoS level as provided by the HIDENETS solutions, adequate **holistic evaluation approaches** have been developed in HIDENETS [6]. The quantitative evaluation of such dependability-related properties is performed following three basic approaches: analytical stochastic modelling, simulation**,** and experimental measurements. Each approach shows different characteristics, which determine the suitability of the method for the analysis of a specific system aspect. The most appropriate method for quantitative assessment depends upon the complexity of the system, its development stage, the specific aspects to be studied, the attributes to be evaluated, the accuracy required, and the resources available for the study. The challenging aspects that characterise HIDENETS, like heterogeneity, dynamicity, variety of threats and mobility aspects cannot be addressed by a single evaluation technique. Therefore, the individual techniques have been developed having in mind how they can be positioned inside the holistic framework.

Hence, the HIDENETS methodological approach follows a holistic philosophy such that the individual evaluation techniques cooperate with each other exploiting their interactions. The individual techniques are introduced as means for evaluating a subset of the HIDENETS scenarios. In the holistic view of HIDENETS, the experimental evaluation techniques and the simulation approaches are used to capture the low level details of the system (at the architecture and communication layers), while the model-based approaches (both analytical and simulative) are used to assess more high-level end-to-end scenarios. Application-specific quantitative analysis of a distributed black-box application, of the platooning use-case, and of an accident use-case have been generalised in a semi-automatic workflow, illustrated in Figure 5.

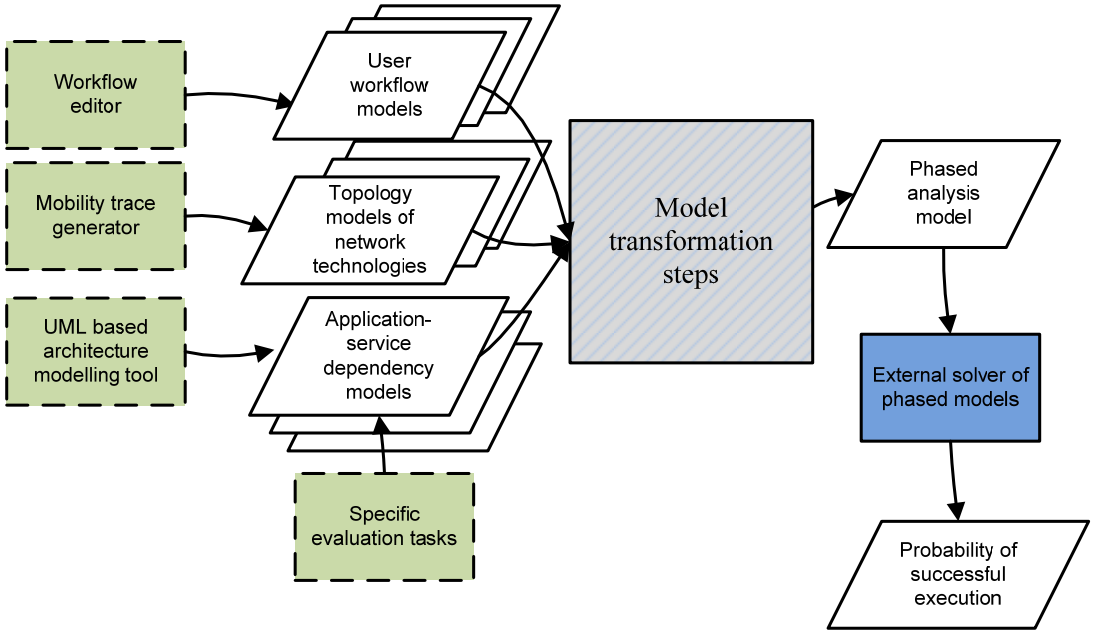


**Figure 5: Inputs and output of the evaluation process**

The implementation of the evaluation workflow allowed us to understand the complexity of evaluating a user level dependability measure in a HIDENETS environment, and contributed to the validation of initial ideas for complexity reduction as well as to the development of techniques for tool integration [21].

Although the HIDENETS project did not develop new applications with high dependability requirements, the application interfaces of the middleware and communication level solutions influence the application development process, hence adequate **development tools** and subsequently **testing methodologies** were developed for applications running on top of the HIDENETS framework [61]: Starting from existing UML meta-models as developed by the *Service Availability Forum*™ (SA_Forum [12]), initial meta-modelling approaches for HIDENETS have been investigated.

Regarding the application interfaces, the SA_Forum standardises the interfaces for systems requiring high levels of service availability. While they focus on the fixed infrastructure domain with predefined clusters, the HIDENETS project aimed at solutions for the ad-hoc domain where clusters are not predefined and change more frequently. The solutions of the SA Forum are re-used in the HIDENETS project in two ways: a.) existing SA Forum compliant middleware has been used on the nodes in the infrastructure domains, and b.) the application programming interface of the HIDENETS platform has been harmonised with the SA Forum standard interfaces.

For what concerns testing aspects, a test strategy based on a dedicated testing platform has been devised to support the black-box testing of mobile applications and middleware services in a simulated environment. It is worth pointing out that the ability to perform such a testing crucially depends on the availability of adequate formalisms for the design and specification of mobile computing systems. As this is still an open research issue, within HIDENETS we have focused on the identification of a special language for expressing candidate test scenarios [61]. What has been pursued is actually a pragmatic approach: the availability of a complete behaviour model is not required, it is only necessary that the user be able to describe scenarios that are deemed important to be tested, and to implement them on the kind of platforms described above.
The application development approach has been validated in an experimental test-bed [20,24], which uses an example application in order to demonstrate (i) the benefits of applying the model driven software engineering methodology and tools developed in the context of HIDENETS “Design methodologies” and (ii) the possibilities for achieving high availability of some key infrastructural services by building them on a standards compliant SA Forum AIS (Service Availability Forum Application Interface Specification) implementation. The chosen application is a prototype Platoon Driver Support System (PDSS) that implements a simplified version of the platooning use-case, while strongly emphasising the development process itself.

The HIDENETS solutions are essential for the deployment of future business-critical applications: the use of off-the-shelf components and wireless communication links will dramatically decrease the costs of market entry and hence make such ubiquitous scenarios commercially feasible. However, these components and communication links are inherently unreliable, and therefore end-to-end system-level resilience solutions addressing both accidental and malicious faults must be developed. The HIDENETS solutions are expected to contribute to a user perception of trustworthiness of future wireless services, as this perception is strongly impacted by availability and resilience aspects. Such perception is critical for the technical and business success of these services. The results show how resilience solutions for new mobility-aware distributed applications with critical dependability requirements can be designed, implemented, and assessed on open communication infrastructures.

# 5. Dissemination and Exploitation Activities

## 5.1 Dissemination

The HIDENETS project had set itself challenging goals, not only with respect to the planned research and development results, but also with respect to the dissemination of the project outcome and uptake of its results by industry and research.

The following key goals were set for the project:

- ✓ Wide communication in scientific and industrial communities,
- ✓ Creating awareness for dependability within a wide audience,
- ✓ Influencing standards evolution in the SA Forum and C2CC Communities,
- ✓ Supporting the technology uptake of the achieved results.

All facets of HIDENETS including the addressed use cases, dependability services, evaluation and development tools as well as the proof of concept prototypes have been presented in a wide set of publications and presentations. Based on the broad expertise of the HIDENETS partners, local audiences as well as international audiences were addressed and could get acquainted with HIDENETS results. In particular the HIDENETS tutorial with its nearly 1000 pages gives an in-depth view of dependability in inherently unreliable environments and related methods, tools and technologies. It is publicly available on the web site for widest use.

From the beginning, the project set a clear focus on two standards organisations it needed to interface with:

- the Service Availability Forum™ (SA Forum, http://www.saforum.org/)
- the Car 2 Car Communication Consortium (C2CCC, http://www.car-to-car.org/)

The SA Forum [12] is a consortium of industry-leading communications and computing companies working together to develop and publish high availability and management software interface specifications. The SA Forum then promotes and facilitates specification adoption by the industry.

The SA Forum is unifying functionality to deliver a consistent set of interfaces, thus enabling consistency for application developers and network architects alike. This means significantly greater reuse and a much quicker turn around for new product introduction.

The SA Forum's mission is to foster an ecosystem that enables the use of commercial off-the-shelf building blocks in the creation of high availability network infrastructure products, systems and services.

Also the standardisation work of C2CCC [13] is industry driven with the automotive industry as its key constituency. The mission and the objectives of the C2CCC are:

- to create and establish an open European industry standard for CAR 2 CAR communication systems based on wireless LAN components and to guarantee European-wide inter-vehicle operability
- to enable the development of active safety applications by specifying, prototyping and demonstrating the CAR 2 CAR system
- to promote the allocation of a royalty free European wide exclusive frequency band for CAR 2 CAR applications
- to push the harmonisation of CAR 2 CAR communication standards worldwide
- to develop realistic deployment strategies and business models to speed-up the market penetration

Project partners are members of the mentioned standards fora and used their influence and contacts to create visibility for HIDENETS project results as well as contribute directly to the standards evolution in the respective consortium. By integrating project results in the work of the standards bodies, it is expected that in future Requests for Quotation or Requests for Proposals as well as in project implementations, dependability aspects will be an explicit mandatory element. For detailed contributions, please see [1].

The Web is used as a global, well accepted means of communication. The HIDENETS web address is http://www.hidenets.aau.dk. The site will be continuously maintained by partner AAU beyond the project duration. It contains all public deliverables for download, papers (typically showing the abstract due to copyright restrictions of the full papers) and presentations, and, last but not least, relevant cross links to the standards fora HIDENETS is interfacing with as well as to related projects with which HIDENETS has established cross linkages.

An important element of the web site is the **HIDENETS Tutorial [23]**, a key tool for the dissemination of HIDENETS results. It covers all project work items in 8 chapters:

0 HIDENETS Introduction
1 Architecture and Use Cases
2 Communication Level Services
3 Middleware and Wormhole Services
4 Model Based Application Development
5 Evaluation
6 Testing
7 Test-Beds
8 Dissemination

The tutorial consists of nearly 1000 slides which were carefully designed to allow easy navigation within the material and have a quick grasp on the work topics and the results. The use of navigation buttons allows walking through the material sequentially and selectively, focusing on only those chapters of interest. The chapters and subchapters have been structured in such a way that the readers can move forward on their individual pace through the slides. With the concept of a short and long version of most subchapters, readers can decide whether they are interested in a more cursory introduction to a certain topic or whether they want to go into details.

## 5.2 Exploitable results

In the sequel, a subset of the exploitable knowledge is discussed focusing on aspects of the key values of the results.

**HIDENETS runtime dependability support**
The HIDENETS run-time dependability support middleware integrates a number of services to be used in high-availability application environments to implement critical dependability properties as required within specific application domains (web applications, telecommunications, telematics and many more). The architecture employs a hybrid design, in which critical parts are executed on a separate computation and communication platform; as a consequence, different execution platforms and different execution environments can be supported.
The following classes of services are included in the dependability support middleware:

1. Timeliness and trustworthiness oracles

   Reliable and Self-Aware Clock
   Duration measurement
   Timely Timing Failure Detection
   Authentication
   Trust and Cooperation Oracle

2. Complex resilience middleware services

   Diagnostic Manager and Reconfiguration Manager
   QoS Coverage Manager
   Intrusion-tolerant agreement
   Cooperative Data Backup
   Proximity Map
   Replication Manager

3. Resilient communication

   Multi-channel multi-radio architecture
   IP resilient routing
   Efficient routing
   Efficient and reliable broadcast
   Resilience in connecting to the infrastructure domain
   Cross-layer optimisation

In addition to the individual services, the ensemble of those in the middleware and their joint use provides higher degrees of resilience. Further, to support the developers of cross-domain applications in the utilization of these middleware services we provided

- a unified access to the services of the dependability support middlewares (both in the ad-hoc and infrastructure domains) and
- model based configuration generation to support the development of cross-domain and multi-platform applications.

For car-to-car and car-to-infrastructure use cases the interaction of the services and the benefits have been illustrated in HIDENETS [20].

**HIDENETS evaluation approach**

The HIDENETS quantitative evaluation approach contains a mixture of pointwise, use case driven, and automated workflow based analysis methods and tools. The approach and the specific realisations can be applied for quantitative analysis of dependability metrics for any system in which mobility is a prevalent characteristic. The application of the approach has been illustrated for certain c2c and c2I use cases in Reference [21].

**Assessment methodology and tool support for evaluation of mobile services in dynamic networking environments**

Communication in wireless networks is affected by uncontrollable disturbances in the channel. Effects of these disturbances are exacerbated in networks with dynamic topologies and multiple hops in end-to-end communication. The lack of control of the channel complicates testing of applications and support functions in such networks as test conditions are hard, or impossible, to reproduce. HIDENETS has developed a methodology and an open-source tool, http://www.sourceforge.net/projects/air-in-a-box, which allows creating reproducible test conditions for such networks by emulating the wireless links. Emulation is performed by a topology emulator testbed to which end-nodes are connected directly using wired links. In real-time, the emulator imposes changing link properties, such as packet loss and delay, onto ongoing traffic between seemingly mobile end nodes. The imposed properties are based on simulations of node mobility, loss and delay models. Evaluation results confirm that the tool is capable of providing link emulation in real time and transparent to the communicating network protocols and applications.

**Tool support for the adaptation process of SA Forum specifications**

Tools have been provided to support the migration of existing and newly developed High Availability services over based middleware implementations based on SA Forum Application Interface Specifications.
Our life increasingly depends on modern telecommunication services and those are strained to their current limits as the doctrine of anytime-anywhere gains more and more significance. The Service Availability Forum™ is a consortium of industry-leading communications and computing companies working together to develop and publish high availability and management software interface specifications to ensure code portability and reduction of development time and cost. The SA Forum then promotes and facilitates specification adoption by the industry.
In the scope of the HIDENETS project the SA Forum specifications were selected for further investigation as possible solution for a standard based implementation of services in the infrastructure domain. The AIS specifications were transformed into a UML profile that serves as a basis for application design within the SA Forum work. Given a properly annotated application model the strengths of the profile can be exploited through the applied stereotypes that highlight the SA Forum relevant traits of the components.

**A framework and mechanisms to support dependable adaptation**

The developed framework is aimed at supporting distributed applications that communicate in probabilistic environments. Moreover, the framework is mainly useful for adaptive applications, which are able to reconfigure some operational parameters (timeouts, buffer sizes, transmission rates, and others) depending on the information provided by the framework. In brief, the framework can be described as a monitoring component that uses input information concerning message round-trip delays, to characterise the behaviour of the network based on that information. Then, based on this characterisation, the framework is able to derive the cumulative probability that message delays will stay bellow some defined value. It will also be able to provide, given some desired cumulative probability, the temporal bound that satisfies this probability. In summary, applications can be developed in a more dependable way, since they will be aware, at any given moment, of the coverage of the parameters used in their operation. For instance, they will know the probability that an expected message will be received before some assumed deadline.
As mentioned above, the framework assumes that message delays follow some probabilistic distribution. Moreover, it assumes that distributions may not be stable over time, but alternate periods of stability with transient periods, during which the probabilistic behaviour cannot be defined. For its correct operation, the framework also needs to receive enough (statistically independent) information about the observed stochastic variable, which necessarily depends on the specific application and on the communication patterns. Finally, it is assumed that the framework is executed in a processing system with enough computational power to support the execution of the selected mechanisms (in fact, the complexity of the involved operations is

sufficiently small for the typical resources available in standard PC infrastructures).
The framework includes a set of mechanisms that allow to: a) detect stable phases regarding the environment behaviour; b) determine different probabilistic behaviours. These mechanisms include two goodness of fit (GoF) tests, namely the Kolmogorov-Smirnov (KS) test and the Anderson-Darling (AD) test, which allow the detection of stable phases for the following probabilistic distributions: exponential, shifted exponential, Pareto and Weibull.
One interesting aspect of the framework is that it can be enriched with additional mechanisms for phase detection, as well as be extended to detect other kinds of probabilistic distributions. This extensibility will allow the framework to continually improve and be able to provide better application support for a wider range of operational environments.
To our knowledge, there are currently no similar frameworks which aim at detecting the probabilistic behaviour of generic probabilistic communication environments and support adaptive applications to achieve better dependability in their operation.

**Distributed black-box application**

A distributed black-box application collects at regular basis time-stamped information on the state of the car running the application and its environment and backs up this information to other neighbouring cars and to fixed network servers. Such information is very valuable, e.g. to support investigations after accidents. This concept is new and has several advantages that will make it attractive to the market: low cost mechanisms for ensuring availability and confidentiality.
The application relies on three main middleware services:

1. *Cooperative data backup:* ensures the replication, scattering, and restoration of critical data in the ad-hoc domain and infrastructure domains. This service can be used in various application areas where data availability and confidentiality need to be ensured in the presence of accidental/malicious threats as well as network disconnections.
2. *Proximity map*: provides a map of neighbouring nodes (along with estimated distance, position and speed). This service can be exploited in any mobile and ad-hoc based application where nodes need to elaborate the local knowledge about their vicinity.
3. *Trust & cooperation*: The goal of this service is to evaluate locally the level of trust of neighbouring entities and to manage cooperation incentives. Our solution is based on the use of middleware certificates and trusted hardware, e.g., a smart-card. It has several advantages: simplicity, efficiency, and it is well suited for the particular case of critical automotive embedded systems.

In the course of the project, no similar application using cooperative backup techniques could be identified in the market yet, especially when applied to black boxes. Black box applications are starting to be deployed by insurance companies. Hence, such application can open new exploitation opportunities in future developments and research, in industry and academia.

**Reliable and Self-Aware Clock (R&SAClock)**
To present the innovative aspects and advantages offered by the R&SAClock, let us consider pervasive, adaptive, open, highly distributed systems (Wireless Sensor Networks, Car-to-Car systems, …). In such systems it is often required that nodes uses clock synchronisation mechanisms to keep their clock synchronised with respect to a global time. However, the time view that a local clock imposes to its node may deviate from global time (some examples of threats to clock synchronisation are unpredictable network delays, unreliable networks, environmental changes, changes in system dynamics, node failures).
Because of these threats to clock synchronisation, the actual distance form global time is a variable factor very hard to predict; moreover worst case bounds on such distance are usually available, since they are imposed to systems as system requirements but these bounds are far from typical execution scenarios and consequently are of practical little use.
Instead the ability to furnish an adaptive conservative estimation on distance of local clock from global time could be useful in a large number of systems. The Reliable and Self-Aware Clock (R&SAClock, [38]) is a brand new technology designed and developed by Università degli Studi di Firenze (UNIFI) that accomplishes this objective, providing more precise and detailed information on distance from global time. It is a new software clock that hides to users the existence of both the synchronisation mechanisms in use (possibly more than one) and the software clock.

The main potential applications of the R&SAClock are in pervasive and adaptive systems (e.g. WSNs, or mobile systems as CAR-to-CAR communication systems), where performances of clock synchronisation mechanisms can be affected by a large set of threats. For example, the R&SAClock can result useful in protocols for localisation of sound sources, where irregular temporal sampling is a problem, and regular temporal sampling is impracticable since requires closely synchronised clocks at all of the measurement points (for example, let us consider sites where GPS access is unavailable, e.g. in woods where there is thick foliage, or in the underground) [60].

# 6 Role of Partners in Consortium

**AAU**

In order to assure the holistic end-to-end approach of HIDENETS, AAU's contributions were intentionally placed on different functionalities on different layers within the HIDENETS run-time solution architecture, in particular covering both communication protocol level and upper-layer middleware. The concepts of distributed server redundancy for infrastructure-based service components have been analysed and integrated in the HIDENETS middleware architecture [45]. The results are optimisation models which allow for offline and run-time enhancement of application-level dependability metrics [45]. Concepts to realise dynamic replication approaches in the ad-hoc domain have been defined and analyzed [46]. The analysis of the performance and resulting dependability is thereby strongly dependent on connectivity properties, both in a static and dynamic setting, for which models in automotive freeway scenarios have been developed and utilised. The experimental analysis of such solutions in dynamic settings has been facilitated by the design and implementation of an emulation tool [47], which has been successfully included in multiple HIDENETS prototypes in order to achieve reproducible experiments. In order to achieve efficient communication in the dynamic ad-hoc domain, enhanced proactive routing protocols with reduced overhead have been developed [48]. The overhead reduction approaches can also be utilised for optimistic broadcast [49] and for reliable broadcast approaches [50]. One particular use-case of reliable broadcast is for geographically bounded hazard warning, for which a cross-layer optimisation architecture and optimisation models for parameter adjustment across Layer 1-3 have been developed [51].

**BME**

In order to support all activities in the traditional Software Development Life-Cycle (SDLC) from application design through development until testing, we opted for a model-based approach in the HIDENETS project. First of all, we had to find a suitable way to support application development in the project domain. Modelling in such emerging and rapidly changing application fields – where widely accepted standards or approaches are unavailable – is always a challenge in itself so after the thorough study of relevant standards we tried to establish a 4-step approach that starts with the underlying concepts and develops them to early design patterns that can be used by designers [52]. That approach can prove to be useful in any innovative environment where the swift introduction of the underlying concepts and the ease of understanding are essential.

We also had to find a suitable solution for operations in the infrastructure domain. As a very important principle during the work was to create standards based solutions wherever possible, we incorporated into the final platform the Service Availability Forum's Application Interface Specification (AIS) to address our experimental needs in that domain. However, being a quite young standard, best practice recommendations for using these interfaces do not exist. A part of the work done was aiming at making it easier for people to understand and use the specifications [53, 54], as well as, providing better tools to facilitate application development [55, 56, 57]. Another aspect that was considered to be very important is the dynamic nature of the HIDENETS platform/environment. Ways have been developed to introduce this feature in the AIS, focusing on the Availability Management Framework [58] which is responsible for the management of application components, and an assessment has been made for the feasibility with currently existing implementations [59].

The testing of mobile distributed applications characterised by high dynamicity raised several challenges which had to be identified and investigated in correspondence with existing UML solutions and possible extensions have been presented [31]. On the other hand, we aimed for user-level evaluation of application scenarios based on a Multi Phased System, taking into account timeliness, spatial attributes and the fault-occurrence probability of underlying hardware implementations and services [36]. In this way, the most relevant aspects of distributed, mobile scenarios over ad-hoc networks could be analyzed in an encompassing way.

**Carmeq**

Carmeq was working in tight cooperation with Volkswagen Research. Technical aspects and features of HIDENETS like the multi-radio multi-channel solution, the broadcast investigations, the abstraction-based modelling approach and the related holistic evaluation workflow were analyzed at Carmeq for exploitation. Carmeq's technical work focused on the development and analysis of vehicular use-cases [3], on the development of predictable Medium-Access Control strategies in vehicular settings, and on the integration of the HIDENETS results in an overall dependability process [22]. Furthermore, Carmeq was one of the key links of HIDENETS into the c2ccc and to other vehicular research projects (e.g., Ref [15]).

**FSC**

The technical work focus of partner FSC (besides the driving the efforts on dissemination, tutorial and business impact analysis and interfacing with the Service Availability Forum) was on the use of standard interfaces and the automation of the development and configuration of standards conformant high-availability systems and applications. For this purpose, FSC worked on the specification of requirements of SA Forum conformant system configurations. These were used as input for the development of platform independent and platform dependent UML models. It was an important to understand the relationship between functions and models as developed by the Service Availability Forum and Hidenets (with a focus on mobile, highly volatile environmental conditions).

Based on these results, partner FSC participated in the development of the application development testbed with a cluster configuration and cluster failover functionality, which showed two very important aspects of Hidenets work:

1. UML Models (a standardised modelling technique widely accepted by industry) have been developed integrating interfaces specified by industry consortia and implemented in an industrial set-up with newly developed advanced functionality from research.
2. Requirements based on the Hidenets focus on mobile, highly volatile environments led to important modelling feedback to the standards body (SAForum).

HIDENETS results are expected to play an important role in future FSC offerings for a number of reasons:
1. High availability and dependability are ubiquitous in today's data center infrastructures. Clustering, fail-over technologies, virtualisation technologies combined with the automation of standard tasks will more and more prevail. Green IT, a long-term strategic goal of Fujitsu Siemens Computers is a key concern and important driver for virtualisation and automation technologies. HIDENETS has made important contributions to the development of run-time services in support of dependability qualities in the data center, a standard FSC offering.
2. At the same time, dependability functions even if standardised (e.g. by SA Forum) increase the complexity of systems and system configurations. Therefore the HIDENETS results on design and development tools as well as test and analysis tools are extremely important for the successful deployment of virtualised, energy efficient data centers or highly dependable solutions.

Because Fujitsu Siemens Computers is focusing on the provision of standardised infrastructures (platform systems and services), the use of standardised functions often coming from OEM partners is a must. Therefore the focus of the FSC involvement in HIDENETS was on the dissemination to standards groups and relevant OEM partners.

**LAAS-CNRS**

One of the solutions investigated in the context of HIDENETS to ensure data protection and resilience against accidental and malicious threats is the provision of an opportunistic cooperative backup service for mobile nodes interacting through unreliable ad-hoc networks and having temporary access to the fixed infrastructure. We have considered the distributed black-box application as a main case study, nevertheless the solutions that we have developed can be applied to other application areas using distributed cooperative data backups in the ad-hoc domain. The design challenges, considering dependability and security related concerns, and the solutions investigated have been discussed in [17, 26]. In addition, we have performed a detailed evaluation study based on analytical modelling that allowed us to have a better understanding of the scenarios where the cooperative backup service yields noticeable data dependability improvement compared to scenarios that do not rely on data backups in the ad-hoc domain [27]. The results give useful insights for tuning the parameters characterizing the distributed black box application depending on the characteristics of the operational environment. Evaluation based on experimental measurements has been also considered in the context of the project. As discussed in [28, 29] such kind of evaluation raises several challenges in particular when experiments are run in a laboratory set up, that need to be addressed carefully in order to provide results that are representative of operational environments.

Besides the evaluation of the distributed black-box application, we have also developed analytical models that allowed us to perform some sensitivity analysis studies with respect to data availability and data consistency in the context of services replicated on mobile nodes [30]. Such analysis has been further explored by integrating some connectivity parameters characterizing typical dynamic vehicular scenarios that have been estimated based on simulation experiments.

Another significant contribution in the context of HIDENETS concerns the development of new methodologies that are well suited for the verification of HIDENETS-like applications and middleware services. The testing of mobile distributed applications characterised by a high dynamicity raised several challenges as discussed in [31] considering as an example a distributed group membership protocol. Our work has then been focused on the definition of a scenario-based testing framework with two main contributions [32]: i) the definition of a language that describes interaction scenarios in mobile settings, and ii) some automated support to analyze and implement scenarios on a test platform with simulation facilities.

**Telenor**

As a telecom network operator, with main operation within mobile area, Telenor will first of all be interested in results related to mobile nodes interconnection to infrastructure networks. One central idea is Always Best Connected. In some of our operations we also have a fixed network, and in Norway we are the major player not only in mobile communications, but also in fixed operations like telephony and broadband (ADSL). We also have public WiFi zones. In this setting we are interested in offering our customers a seamless Internet access across the different technologies, with high availability, such that our customers anywhere can use the access technology most useful for their needs. In this setting HIDENETS results related to Infrastructure access ([5], [62]) will be further exploited.

Some of the HIDENETS applications will have stringent requirements on the robust delivery of data, either due to a real-time nature of the application or due to the importance of the content. These In the ad-hoc domain these applications bring challenges to the routing protocols due to the failure frequency of wireless links and possible mobility of nodes. A considerable amount of these failures are transient, meaning that the links and nodes may return to normal operation and position within short time. In such scenarios, routing protocol actions like re-convergence of routing state may cause instability and unnecessary bandwidth consumption. In [33], we introduced an approach using multi-topology routing for increasing the resilience in wireless networks. In [34], we demonstrated that this multi-topology routing can also guarantee recovery from multiple concurrent failures. We are not aware of any other scheme that can guarantee this in connectionless IP networks. In [35], we have presented an extensive evaluation of our routing approach in different scenarios. We have compared performance and functional properties with several other schemes. Our conclusion is that our routing scheme seems to be the best candidate in the scenarios evaluated in [35].

**FCUL**

The work developed in the context of HIDENETS has focused on architectural aspects, in particular on the application of the architectural hybridisation concept to the development of the system architecture, and on the development of services for improved resilience (timeliness and security). The overall results have been applied in the development of the Platooning application test-bed. The fundamental concepts concerning architectural hybridisation have been published in earlier papers and some specific implementation aspects of the construction of an embedded wormhole, which materialises the concept, have been published in [44]. Security aspects concerning intrusion-tolerant protocols and their application in ad-hoc environments have been developed and analyzed in [42], while a particular extension to these protocols that considers the possibility of using reliable services in the infrastructure domain has been addressed in [43]. In these works it is shown that despite the complexity and overhead of the solutions needed to achieve consensus in ad-hoc networks in the presence of byzantine attackers, the proposed solutions could be used in practical scenarios. The problem of dependably monitoring the latency of the communication system, so that adaptation decisions can be taken with known dependability levels has been addressed in [39]. We proposed a framework that is aimed at probabilistic environments and which allows several techniques to be used in parallel in order to detect the actual probabilistic state of the environment and, hence, better support adaptation decisions. Finally, the developed Platooning test-bed, and the several proof-of-concept scenarios that were demonstrated in this test-bed, is addressed in [40].

**WMC**

The work of WMC has focussed on the resilience at the communication layer and on the prototyping and validation of some of the solutions developed in the context of HIDENETS. In particular, WMC investigated the potentials of multi-channel/multi-radio communications in car-to-car environments, with a strong focus on robust channel selection algorithms. The work included analysis, simulations, and experimental research and it was complemented with an analysis of the cross-layer relations between the multi-channel multi-radio component and other components of the HIDENTS architecture including potential cross-layer optimisations. The results obtained in HIDENETS have shown the benefits of the proposed architecture in mobile (vehicular) environments, especially when using multi-hop communication.

.From the point of view of exploitation, the results obtained in HIDENETS are very important for WMC. In its 6 years of existence, WMC has developed as the “Home of Wireless Ad-hoc Radio Networks” in The Netherlands. Since recently, our company has extended its activities in contract research and consultancy with the development of professional wireless mesh products for vehicles. The knowledge on resilient connectivity gained in HIDENETS will give WMC an advantage for the development of innovative wireless networking communication products for transportation and safety-critical applications.

In particular, the following results of HIDENETS offer potential for exploitation:

- Multi-radio/multi-channel routing algorithms for dependable communication in multi-hop ad-hoc networks
- Algorithms for radio channel assignments in multi-channel/multi-radio multi-hop ad-hoc networks
- Algorithms and protocols for gateway/network selection and multi-homing in connecting ad-hoc vehicular networks to the infrastructure

WMC will use the project results in two projected product lines. The first product line is FIGO. It targets the professional market with high-end communication products that fulfil all communication needs in high demanding emergency relief. Based on the experience in the professional market, a second product line will target the mass market consumer application. WMC foresees a communication need in the automotive environment for the consumer and semi-professional sectors matched by these products.

**UNIFI**

In [36] and [37] we have introduced two modelling methodologies for QoS and dependability evaluation in mobile, heterogeneous and dynamic distributed environments. In [36] we have proposed a model-based approach that, through a sequence of model transformation steps, automatically derives the Multiple Phased System model representing the analyzed mobile scenario starting from high-level UML specifications. In [36] the focus was on the QoS analysis of a dynamic, ubiquitous UMTS network scenario taking as motivating example a subset of the “car accident” use-case scenario developed in WP1. Adopting a compositional modelling approach based on Stochastic Activity Networks formalism, we have analyzed the QoS both from the users’ perspective and from the mobile operator’s one.

Specific HIDENETS middleware components have been proposed and evaluated in [38] and [39]. The Reliable and Self-Aware Clock (R&SAClock), a low-intrusive software service that is able to compute a conservative estimation of distance from an external global time, has been proposed in [38]. R&SAClock acts as a new clock that couples information gained from synchronisation mechanisms with information collected from the local clock to provide both current time and a self-adaptive reliable estimation of distance from global time. In [39] the focus was on the definition of concrete strategies and methodologies to improve the implementation of dependable QoS adaptation, which is the capability of distributed protocols to adapt dynamically to environment changes in order to preserve QoS.

# 8 Further work

The need for dependability solutions will continuously advance due to the overall pervasive introduction of distributed computing systems in almost all areas of life. Therefore HIDENETS solutions can and will be adapted to various domains and application fields in our all-day life. Typical domains are e.g. remote health monitoring public transportation systems, the financial sector, embedded systems like train control systems and public safety and disaster relief. This section describes some examples of where to apply these solutions.

### Public safety and disaster relief

The results achieved in HIDENETS are of relevance for public safety and crisis management applications. Dependability of services and reliable and efficient communication are crucial for crisis management in man-made or natural disasters.

Traditional systems have shown major limitations in disasters as 9/11, hurricane Katrina, and the bombing in the London metro. One of the major problems had to do with the strong reliance on services offered by the infrastructure, and in particular on terrestrial communication facilities. The operation of the first responders was severely hampered when the infrastructure was damaged or overloaded.

These problems have been recognised and large initiatives have been launched to address the shortcomings of current public safety and disaster recovery systems. Examples are the US SAFECOM project and the North American/European MESA programme that, amongst many other results, have proposed an architecture and a set of requirements for next generation systems. The architecture reflects the hierarchy of the command and control structure and contains infrastructure as well as ad-hoc components. Requirements such as high availability, security, mobility support, robustness, and quality of service are considered essential. The architecture as well as the requirements have a lot in common with HIDENETS and it is very likely that this field could largely benefit from the results of the project.

In particular, the results of HIDENETS on multi-homing, multi-radio communication, distributed back box, and replication servers are very relevant for this application area. It is worth mentioning, that domain specific issues, as the use of dedicated radio technologies, different mobility models, connectivity patterns that reflect the command hierarchy, strong security requirements, prioritizing of traffic, and different applications require modifications and extensions of the HIDENETS results before being directly applicable to this area.

### Car-to-home and car-to-mobile device

HIDENETS solutions are developed for car-to-car and car-to-infrastructure scenarios and can be adapted to car-to-home and car-to-mobile device scenarios which are scenario subsets of the overall car-to-x domain.

Similar to HIDENETS scenarios car-to-home scenarios deal with up and downloads of documents, multimedia streaming and data synchronisation of navigation and remote control information. In an exemplary situation a user prepares a longer trip and uploads helpful documents from the home computer to the car like navigation maps, trip routes or audio books.

Other car-to-home use cases discussed in the automotive domain overlap with car-to-infrastructure use cases and are related to applications and needs which are mainly showing up during a trip (e.g. instant messaging).

More abstract, from a communication perspective car-to-home is focused on connecting a driver's home infrastructure with his/her car. This can be realised through a connection between the car and a standard WLAN router placed at home, via UMTS, or car to Road Side Unit communication. The selection of the most appropriate technology depends on the use case scenario in question, the on-board equipment, the resulting communication costs, and the distance between home and car. These conditions can be integrated to the always-best-connected principle of HIDENETS. Most of the use cases can be processed over a one or multi hop connection while the car is parking nearby in the neighbourhood. Hereby, HIDENETS solutions like resilience routing and fast IP rerouting are suitable to be adapted to this particular situation in which passing vehicles can be used for packet forwarding. In conclusion, car-to-home scenarios demand the dependability solutions developed in HIDENETS and additionally focus more on privacy and security requirements.

The second mentioned scenario subset is called car-to-mobile device in which e.g. laptops or mobile phones placed in the car are connected to the car. These devices can be connected via Bluetooth, USB, or Firewire e.g. to take advantage of the on-board communication technologies. For instance, passengers could use applications on their laptop which need to be online and therefore utilise fully the HIDENETS always best

connected principle integrated in the car. This way the car is a mobile router for external applications and devices. Moreover, these external applications can use the HIDENETS middleware and wormholes services (e.g. via SA Forum interfaces).

## Trustworthy network infrastructures

HIDENETS solutions will be relevant when developing solutions for the Future Internet[1] with focus on trustworthy network infrastructures. Methods have been studied within HIDENETS for resilience when connecting to infrastructure networks with the aim of being Always Best Connected. Further work is required for smart access point selection and mobility management.

Solutions that support communication resilience based on wireless network diversity will be of profound importance for operators in the future. Terminals should be enabled to access the Internet anytime and everywhere, using a variety of applications, and should have the possibility for swapping between different networks and using different technologies depending on application demands, cost etc. Due to the inherent unreliability and continuously changing conditions, resilient solutions are sought for. Resilience and QoS differentiation is necessary to prioritise critical applications when parts of the network are exposed to failure.

Also cross-layer design to handle the heterogeneity and dynamics associated with such network scenarios will be of importance. In this context, protocol design (new protocols or modification of existing protocols) from the link level to the transport level are of special interest, but also the design of application specific architectures and middleware solutions.

[1] Future Internet is a general term for work addressing solutions for a next generation Internet

# 9 Project information

Contact information

**Project Co-ordinator**
Assoc. Prof. Hans-Peter Schwefel
Aalborg University, 9220 Aalborg East, Denmark, Tel +45 9940 8677, hps@es.aau.dk, http://kom.aau.dk/~hps
Forschungszentrum Telekommunikation Wien – ftw, Donau-City Str. 1, 1220 Wien, Austria, schwefel@ftw.at

**Adm. Project Manager**
Lone Varn Johannsen, Aalborg University - Fundraising & Project Management Office, Niels Jernes Vej 10 (A 1st west), 9220 Aalborg E, Denmark, Phone: +45 99407275, Fax: +45 9815 7331
lvj@adm.aau.dk <mailto:lvj@adm.aau.dk - www.funding.aau.dk/ <http://www.funding.aau.dk/>

**Dissemination and Exploitation Leader:**
Dr. Manfred Reitenspiess, Director Business Development Strategic Accounts, Fujitsu Technology Solutions, Mies-van-der-Rohe-Straße 8 D-80807 Muenchen Germany, Tel. +49 89 3222 1892, mbl: +49 171 7636290,
manfred.reitenspiess@ts.fujitsu.com

Project Homepage
www.hidenets.aau.dk

# 10 Selected References

[1] HIDENETS web-page: http://www.hidenets.aau.dk
[2] J. Arlat, M. Kaaniche (eds.): 'HIDENETS – revised reference model'. HIDENETS consortium, Deliverable D1.2, online available at http://www.hidenets.aau.dk/Public+Deliverables, June 2007.
[3] M. Radimirsch (ed.): 'HIDENETS – Use-case scenarios and preliminary reference model.' HIDENETS consortium, Deliverable D1.1, available at http://www.hidenets.aau.dk/Public+Deliverables, Sept 2006.
[4] A. Casimiro (ed.): 'HIDENETS – resilient architecture (final version)' HIDENETS consortium, Deliverable D2.1.2, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2007.
[5] I. Svinnset (ed.): 'HIDENETS – resilient topologies and routing (final version)' HIDENETS consortium, Deliverable D3.1.2, available at http://www.hidenets.aau.dk/Public+Deliverables, June 2008.
[6] P. Lollini, A. Bondavalli (eds.): 'HIDENETS – Identification and development of evaluation methodologies, techniques, and tools (final version)', HIDENETS consortium, Deliverable D4.1.2, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2007.
[7] P. Lollini, A. Bondavalli (eds.): 'HIDENETS – Application of the evaluation framework to the complete scenario (Preliminary Version)', HIDENETS consortium, Deliverable D4.2.1, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2007.
[8] A. Kovi (ed.): 'HIDENETS – UML profile and design patterns library (preliminary version)' HIDENETS consortium, Deliverable D5.1.1, available at http://www.hidenets.aau.dk/Public+Deliverables, March 2007.
[9] H. Weaselynck, Z. Micskei, M.D. N'Guyen, N. Riviere: 'HIDENETS -- Preliminary Testing Framework and Methodology', HIDENETS consortium, Deliverable D5.2, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2007.
[10] I. de Bruin (ed), 'Specification of HIDENETS laboratory set-up scenario and components', HIDENETS consortium, Deliverable D6.2, available at http://www.hidenets.aau.dk/Public+Deliverables, Oct 2007.
[11] HIDENETS conference and journal publications: references and abstracts available at http://www.hidenets.aau.dk/Papers+%26+Presentations/1245038. Full papers available at conference/journal web-site or upon request to authors.
[12] Service Availability Forum: http://www.saforum.org
[13] Car-to-Car Communication Consortium: http://www.car-to-car.org/
[14] Cooperative Systems for Intelligent Road Safety (COOPERS), FP6 Integrated Project, www.coopers-ip.eu
[15] Communications for eSafety –COMEsafety. FP6 Specific Support Action, www.comEsafety.org
[16] A. Casimiro (ed.) 'Service level resilience solutions for the infrastructure domain' HIDENETS consortium, Deliverable D2.2 available at http://www.hidenets.aau.dk/Public+Deliverables, June 2008
[17] A. Casimiro (ed.) 'Service level resilience solutions for the ad-hoc domain' HIDENETS consortium, Deliverable D2.3, available at http://www.hidenets.aau.dk/Public+Deliverables, June 2008
[18] J. Nielsen (ed.) 'Cross-Layer Resilience Optimisation in the Ad-Hoc Domain' HIDENETS consortium, Deliverable D3.2, available at http://www.hidenets.aau.dk/Public+Deliverables, June 2008
[19] L. Fallalai (ed.)'Mechanisms to provide strict dependability and real-time requirements' HIDENETS consortium, Deliverable D3.3, available at http://www.hidenets.aau.dk/Public+Deliverables, June 2008
[20] Z. Egel (ed.) 'Documentation and Evaluation of the experimental work' HIDENETS consortium, Deliverable D6.4, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2008.
[21] P. Lollini, A. Bondavalli (eds.) 'Application of the evaluation framework to the complete scenario' HIDENETS consortium, Deliverable D4.2.2, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2008.
[22] B. Könning (ed.) 'Final evaluation, consolidated results and guidelines' HIDENETS consortium, Deliverable D1.3, available at http://www.hidenets.aau.dk/Public+Deliverables, Jan 2009.
[23] M. Reitenspiess, S. Orban (eds.) 'HIDENETS Tutorial' HIDENETS consortium, Deliverable D7.3, available at http://www.hidenets.aau.dk/Public+Deliverables, Oct 2008.
[24] M. Reitenspiess (ed.) 'Experimental proof-of-concept up HIDENETS' HIDENETS consortium, Deliverable D6.3, available at http://www.hidenets.aau.dk/Public+Deliverables, Aug 2008
[25] L. Courtès, M-O. Killijian, D.Powell. Storage Tradeoffs in a Collaborative Backup Service for Mobile Devices, In: Proc. 6th European Dependable Computing Conference (EDCC-6), Coimbra, Portugal, October 18-20, IEEE Computer Society, 2006.

[26] L. Courtès, M-O. Killijian, D. Powell. Security Rationale for a Cooperative Backup Service for Mobile Devices, In: Proc. 3rd Latin American Symposium on Dependable Computing (LADC 2007), Morelia, Mexico, September 26-28, IEEE Computer Society, 2007.
[27] L. Courtès, O. Hamouda, M. Kaâniche, M-O. Killijian, D. Powell. Dependability Evaluation of Cooperative Backup Strategies for Mobile Devices, In: Proc. 13th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'07), Melbourne, Victoria, Australia (PRDC'07), Melbourne, Victoria, Australia, December 17-19, IEEE Computer Society, 2007.
[28] M.O. Killijian, N. Rivière, M. Roy, Experimental Evaluation of Resilience for Ubiquitous Mobile Systems, In: Proc. 1st International Workshop on Ubiquitous Systems Evaluation (USE '07) http://www.useworkshop.org/, organised in conjunction with UbiComp-2007 http://www.ubicomp2007.org/, Innsbruck, Austria.
[29] M.O. Killijian, D. Powell, M. Roy, G. Sévérac. Experimental Evaluation of Ubiquitous Systems - Why and how to reduce WiFi communication range, In Proc. 2nd International Conference on Distributed Event-Based Systems (DEBS08) http://debs08.dis.uniroma1.it.
[30] E. V. Matthiesen, O Hamouda, M. Kaâniche, H-P. Schwefel. Dependability Evaluation of a Replication Service for Mobile Applications in Dynamic Ad-Hoc Networks, In Proc. 5th International Service Availability Symposium, ISAS 2008 Tokyo, Japan, May 19-21, Springer, Lecture Notes in Computer Science , Vol. 5017, pp 171-186, 2008.
[31] H. Waeselynck, Z. Micskei, M. D. Nguyen, N. Rivière,. Mobile Systems from a Validation Perspective: a Case Study: In Proc. 6th International Symposium on Parallel and Distributed Computing (ISPDC-2007) Hagenberg, Austria, July 5-8, 2007.
[32] M. D. Nguyen, H. Waeselynck, N. Rivière,. Testing Mobile Computing Applications: Toward a Scenario Language and Tools: In Proc. Sixth International Workshop on Dynamic Analysis (WODA 2008), ACM Press, Seattle, USA, July 21, 2008.
[33] A. F. Hansen, T. Cicic, and P. E. Engelstad. Profiles and Multi-Topology Routing in Highly Heterogeneous Ad Hoc Networks, In: INFOCOM 2006, Poster and Demo session, Barcelona, Spain April 23-29, IEEE, 2006.
[34] A. F. Hansen, O. Lysne, T. Cicic, and S. Gjessing. Fast Proactive Recovery from Concurrent Failures, In: IEEE International Conference on Communications (ICC 2007), ed. by IEEE, IEEE (ISBN: 1-4244-0353-7), 2007.
[35] A. F. Hansen, G. Egeland, and P. Engelstad. Could Proactive Link-State Routed Wireless Networks Benefit from Local Fast Reroute?, In: 6th annual Communication Networks and Services Research Conference, 2008. CNSR 2008, ed. by Patrick Kellenberger - IEEE, pp. 453-462, IEEE (ISBN: 978-0-7695-3135-9), 2008.
[36] M. Kovács, P. Lollini, I. Majzik, A. Bondavalli. An Integrated Framework for the Dependability Evaluation of Distributed Mobile Applications. In Proc. of the RISE/EFTS Joint International Workshop on Software Engineering for Resilient Systems (SERENE 2008), Newcastle upon Tyne (UK), November 17-19, 2008.
[37] A. Bondavalli, P. Lollini, L. Montecchi. Analysis of User Perceived QoS in Ubiquitous UMTS Environments Subject to Faults. In Proc. of the 6th IFIP Workshop on Software Technologies for Future Embedded & Ubiquitous Systems (SEUS 2008), Capri Island, Italy, October 1-3, 2008.
[38] A. Bondavalli, A. Ceccarelli, L. Falai. Assuring Resilient Time Synchronisation. In Proc. of the 27th International Symposium on Reliable Distributed Systems (SRDS 2008), Napoli, Italy, October 6 – 8, 2008.
[39] A. Casimiro, P. Lollini, M. Dixit, A. Bondavalli, P. Veríssimo. A framework for dependable adaptation in probabilistic environments. In Proc. of the 23rd ACM Symposium on Applied Computing (SAC 2008), Dependable and Adaptive Distributed Systems (DADS) Track, pages 2192-2196, Fortaleza, Ceara, Brazil, March 16 - 20, 2008.
[40] Luis Marques, Antonio Casimiro. Design and development of a proof-of-concept Platooning application using the HIDENETS architecture. In Proc. of the 39th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-2009), June 28 - July 2, 2009, Estoril, Portugal.
[41] TACID: Timely ACID Transactions; (http://gbd.dei.uc.pt/view_project.php?id_p=55
[42] Henrique Moniz, Nuno F. Neves, Miguel Correia, António Casimiro and Paulo Verissimo. Intrusion Tolerance in Wireless Environments: An Experimental Evaluation. Proceedings of the 13th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'07), Melbourne, Victoria, Australia,

December 2007.
[43] Hans P. Reiser and António Casimiro. Optimizing Byzantine Consensus for Fault-Tolerant Embedded Systems with Ad-Hoc and Infrastructure Networks. 4th International Workshop on Dependable Embedded Systems (WDES'07), Bejing, China, October 2007.
[44] Hugo Ortiz, António Casimiro and Paulo Veríssimo. Architecture and Implementation of an Embedded Wormhole. In Proceedings of the 2007 Symposium on Industrial Embedded Systems (SIES'07), Lisbon, Portugal, July 2007.
[45] T. Renier, A. Daidone, HP Schwefel, A. Bondavalli ,Optimal Configuration of Fault-Tolerance Parameters for Distributed Replicated Server Access. Submitted.
[46] E. Matthiesen, O. Hamouda, M. Kaaniche, H-P Schwefel, 'Dependability Evaluation of a Replication Service for Mobile Applications in Dynamic Ad-Hoc Networks' International Service Availability Symposium (Proceedings to appear in Springer LNCS), Japan, 2008.

[47] A. Nickelsen, M. Jensen, E. Matthiesen, HP Schwefel. Scalable Emulation of Dynamic Multi-hop Topologies. 4th International Conference on Wireless and Mobile Communications (ICWMC), 2008.
[48] Y. Liu, F. Li, A. Nickelsen, HP Schwefel 'A new Link State Routing Protocol for Mobile Ad-hoc Networks', 4th IEEE International Symposium on Wireless Communication Systems (ISWCS), 2007.
[49] Y. Liu, HP Schwefel, Algorithms for Efficient Broadcasting in Wireless Multi-hop Networks, Proceedings of IEEE Globecom, 2006.
[50] Y. Liu, F. Li, HP Schwefel, Reliable Broadcast in Error-Prone Multi-hop Wireless Networks: Algorithms and Evaluation, Proceedings of IEEE Globecom 2007.
[51] J. Nielsen, J. Grønbæk, T. Renier, HP Schwefel, T. Toftegaard, Cross-Layer Optimisation of Multipoint Message Broadcast in MANETs. Proceedings of WCNC 2009.
[52] Gergely Pinter, Zoltan Micskei, Andras Kovi, Zoltan Egel, Imre Kocsis, Gabor Huszerl and Andras Pataricza. Model-Based Approaches for Dependability in Ad-Hoc Mobile Networks and Services. In R. de Lemos, F. Di Giandomenico, C. Gacek, H. Muccini and M. Vieira (Eds.) Architecting Dependable Systems V (LNCS-5135). 2008, Springer
[53] András Kövi, Dániel Varró, Zoltán Németh: Making Legacy Services Highly Available with OpenAIS: An Experience Report. ISAS 2006: 206-216
[54] Z. Micskei, I. Majzik, F. Tam: Comparing Robustness of AIS-Based Middleware Implementations, In Proceedings of International Service Availability Symposium (ISAS 2007), LNCS 4526, Durham, New Hampshire, USA, May 21-22, 2007.
[55] András Kövi, Dániel Varró: An Eclipse-Based Framework for AIS Service Configurations. ISAS 2007: 110-126
[56] Zoltan Szatmari, Andras Kovi and Manfred Reitenspiess. Applying MDA for SA Forum AIS based application development. MAI2008 workshop at DisCoTec2008
[57] Z. Szatmári, "Model-driven development for highly available serices", 2008
[58] Gábor Urbanics, András Kövi, Zoltán Égel, András Pataricza. Introducing dynamism to SA Forum cluster, DNCMS08 workshop at SRDS2008.
[59] G. Urbanics, "Introducing dynamism to SA Forum cluster", MSc Diploma thesis 2008
[60] D. Ganesan, S. Ratnasamy, H. Wang, and D. Estrin. Coping with irregular spatio-temporal sampling in sensor networks. SIGCOMM Comput. Commun. Rev., 34(1):125–130, 2004
[61] G. Huszerl (ed.): 'HIDENETS – Refined design and testing framework, methodology and application results' HIDENETS consortium, Deliverable D5.3, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2008.