Publishable executive summary

HIghly-DEpendable ip-based NETworks and Services – HIDENETS

HIDENETS is a Specific Targeted Research Project (STREP) in the European 6th Framework Program. The project has started January 2006 with three years duration. Its objective is to develop and analyze 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. The solution development and analysis require a holistic approach combining aspects of communications, middleware, service deployment and access. Hence the research work combines 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), see http://www.hidenets.aau.dk [1] for more detailed partner descriptions.

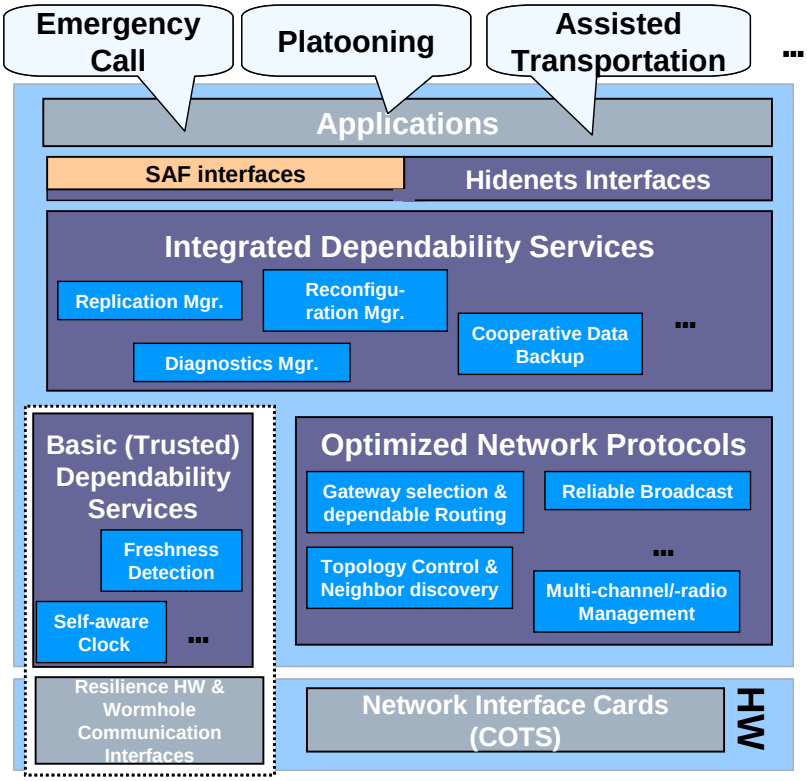

Figure 1: HIDENETS dependability architecture including a subset of the functionalities developed in the project; for a complete list see References [2] and[4]. The dark shaded architecture parts mark the technical scope of HIDENETS.

HIDENETS addresses the provision of available and resilient distributed applications and mobile services in highly dynamic environments characterized by unreliable communications and components due to the occurrence of accidental and malicious faults (attacks and intrusions). 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, are used as driving examples to identify the key features (challenges, threats, and resilience requirements) that are relevant in the context of the project. Based on these features, the project develops appropriate fault-prevention and faul-tolerance mechanisms at the middleware and communication layers, as well as methodologies to support the design, development, evaluation, and testing of dependable solutions using such mechanisms.

Figure 1 shows the architecture and a subset of the dependability related functions that are being developed in HIDENETS. The main elements of this architecture are:

- Middleware dependability services: These functions enable fault-prevention 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] for more details. Some of these functionalities need to be accessed by the applications. Although standardized interfaces [9] are utilized as far as possible, specific functions addressing the dynamicity of the ad-hoc networking scenario require the specification of additional interfaces [2,7].
- 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 [2,5] 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 1. The architectural separation is also applied to the communication functions and interfaces for these distributed dependability services [2,4].

The developed resilience solutions are being analyzed in HIDENETS in a holistic evaluation framework [6], utilizing analytic models and simulation approaches as well as experimental measurements, see Reference [7] for preliminary evaluation results. Furthermore, a methodology is being elaborated to support the testing of application components and middleware services taking into account the challenges raised by mobility [9]. Through the use of UML based design methodologies, the application development on top of the HIDENETS middleware and communication services will be facilitated [8]. A set of experimental testbeds is being developed to validate the key concepts of the HIDENETS resilience solutions [10]: Prevention and tolerance to timing and crash faults of the ad-hoc communication links and multi-hop paths, redundant data storage and application execution in the dynamic ad-hoc domain, assurance of timeliness properties and timely reaction to their violations in the context of a safety-critical platooning application, application development and use/configuration of infra-structure based high-availability clusters [12] for resilient car-to-car c2c and car-to-infrastructure c2I applications.

The research work for HIDENETS is performed in close collaboration with members of the Service Availability Forum [12] and of the Car-2-Car Communication Consortium [13] in order to assure the practical relevance of the research results and in order to stimulate industry interest beyond the members of the HIDENETS consortium. Furthermore, the HIDENETS project is also linked with several other European Research initiatives, see [1] for details.

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 final result will show how resilience solutions for new mobility-aware distributed applications with critical dependability requirements can be designed, implemented, and assessed on open communication infrastructures.

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 (preliminary version)' HIDENETS consortium, Deliverable D3.1.1, available at http://www.hidenets.aau.dk/Public+Deliverables, Dec 2006.
[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/

Consortium

Participant name	Participant short name	Country
Aalborg University, Center for TeleInFrastruktur (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

Contact information

Project Co-ordinator
Assoc. Prof. Hans-Peter Schwefel, Aalborg University, 9220 Aalborg East, Denmark, Tel +45 9940 8677, hps@kom.aau.dk - <http://kom.aau.dk/~hps>

Adm. Project Manager
Peter Ebbe Holm, Aalborg University - Fundraising & Project Management Office, Niels Jernes Vej 10 (A 1st west), 9220 Aalborg E, Denmark, Phone: +45 9940 7255, Fax: +45 9815 7331
peh@adm.aau.dk - <http://www.funding.aau.dk/>

Dissemination and Exploitation Leader:
Dr. Manfred Reitenspiess, Director Strategic Accounts Business Development Services, Fujitsu Siemens Computers, Domagkstr. 28 D-80807 Muenchen Germany, Tel. +49 89 3222 1892, mbl: +49 171 7636290
manfred.reitenspiess@fujitsu-siemens.com

Project Homepage

http://www.hidenets.aau.dk