European Commission

This fiche is part of the wider roadmap for cross-cutting KETs activities

'Cross-cutting KETs' activities bring together and integrate different KETs and reflect the interdisciplinary nature of technological development. They have the potential to lead to unforeseen advances and new markets, and are important contributors to new technological components or products.

The complete roadmap for cross-cutting KETs activities can be downloaded from:

http://ec.europa.eu/growth/industry/key-enabling-technologies/eu-actions/ro-ckets

Potential areas of industrial interest relevant for cross-cutting KETs in the Electronics and Communication Systems domain

This innovation field is part of the wider roadmap for cross-cutting KETs activities developed within the framework of the RO-cKETs study. The roadmap for cross-cutting KETs activities identifies the potential innovation fields of industrial interest relevant for cross-cutting KETs in a broad range of industrial sectors relevant for the European economy.

The roadmap has been developed starting from actual market needs and industrial challenges in a broad range of industrial sectors relevant for the European economy. The roadmapping activity has focused on exploring potential innovation areas in terms of products, processes or services with respect to which the cross-fertilization between KETs can provide an added value, taking into account the main market drivers for each of those innovation areas as well as the societal and economic context in which they locate.

Taking the demand side as a starting point, cross-cutting KETs activities will in general include activities closer to market and applications. The study focused on identifying potential innovation areas of industrial interest implying Technology Readiness Levels of between 4 and 8.

E&C.4.7: Dependable communication platforms and IT infrastructures

Scope:

To build secure and dependable communication platforms and Information Technology (IT) infrastructures and services, relying on cryptography, authentication, authorization and accounting methods, deperimeterized firewalling, pro-active STDP (security, trust, dependability and privacy) solutions, physical hardening, etc.

Demand-side requirements (stemming from Societal Challenges) addressed:

- Inclusive society is also about closing the digital divide (according to the Digital Agenda for Europe (DAE), 78% of EU citizens use the internet at least once a week, 20% never used the internet, and 62% of the EU has 30Mbps broadband, but only 18% of rural areas). Skills or network deployment are to be supported, but technological developments are required in broadband wireless communications, very high broadband wireline communications, networks interfacing and systems autonomous connectivity, user-friendliness
- With ubiquitous digitalization, cyber-security and protection of the communications is a crucial contributor to a safe EU secure and free society
- Improved transport and energy services, as well as all sorts of system monitoring services (environment monitoring, homeland surveillance, industrial supply chains, etc.) all rely on ever-growing flows of digital information, increasing the need for reliable high throughput communication networks
- Information and communication technologies consume around 2% of global energy consumption, and this is the sector with the fastest growth over past and probably upcoming years. Increasing energy efficiency in Information and Communication Technology (ICT) is crucial

Demand-side requirements (stemming from market needs) addressed:

- Volumes of data exchanges have been continuing growth in the recent years, while European telecommunication operators have been experiencing a drop. These operators expect improved communication networks to provide them with capabilities for new services and constitute important growth and profitability relays
- Normalization is a very important driver or barrier for telecom-related industrial activities. Being at the top-front of innovation in low layer telecoms often provides a direct competitive advantage
- Concern is growing in society about electromagnetic waves. In the meanwhile, the radiofrequency spectrum is a limited resource more and more intensively exploited. Optimizing wireless networks for minimizing resource use and possible health impacts is getting more and more important

Specific technical/industrial challenges (mainly resulting from gaps in technological capacities):

- Provision of services and their content securely between all users by high-performing cryptographic methods, including low cost low power highly secure hardware-based cryptographic protection of networks (“cryptographic key”) and systems for payment and micropayment
- Replacement of network securing by platform securing, so as to ensure deperimeterized architecture firewalling (protection against attacks) and antivirusing (against malicious code)
- Development of methods for authentication, authorization and accounting (AAA) while tackling privacy issues
- Mutual authentication of user device and the network based on identity management, including terminal biometrics
- Development of technology to offer appropriate and fair protection to those who wish to retain a degree of control over content they have created or acquired (including the right to remuneration) when it is distributed over heterogeneous networks
- Development of industrial strength methods, metrics and tools for security assurance, forensics and vulnerability discovery
- Development of alternative self-organizing and reconfigurable and/or defect- and fault tolerant architectures and related hardware technologies
- Limitation of intrusion possibilities using near field communication (incl. Radio-frequency identification, RFID), device-to-device communication, secure protocols and low power consumption self-node’s integrity validity check

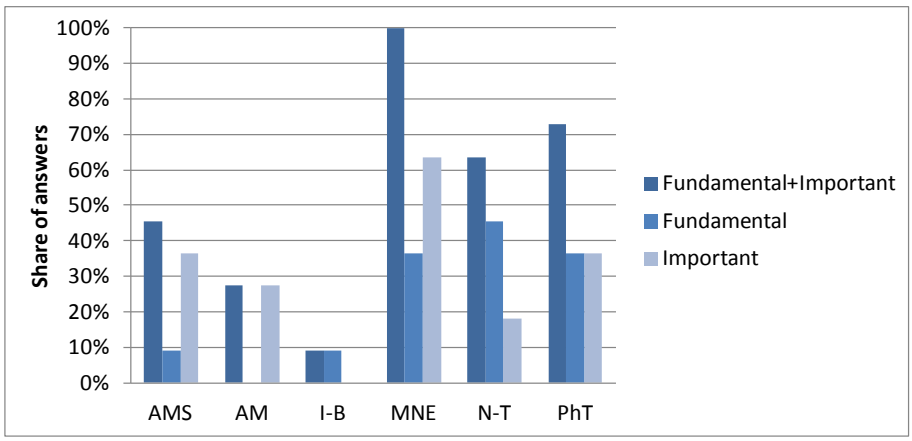
- Setup of proactive network surveillance capabilities to detect and track malicious users of (mainly wireless) networks, and trigger counter intrusion or self-healing measures, including STDP solutions (security, trust, dependability and privacy)
- Support of network management software controlled by European players and/or open source
- Guarantee sufficient supply of rare raw materials, especially rare earths, or develop synthetic equivalent
- Ensure trustworthy record, storage, transfer and usage of personal data, so as to prevent new types of attacks, privacy breaching or technology-induced safety risks
- Development of hardened components, including memories
- Increase of modularity, scalability and interoperability of data server modules

Contribution by cross-cutting Key Enabling Technologies:

In respect to this Innovation Field, the integration of KETs could contribute to the development of secure and dependable communication platforms and IT infrastructures and services, relying on hardware-based cryptographic protection, authentication, authorization and accounting, limitation of intrusion, device-to-device communication, self-organizing and reconfigurable, defect and fault tolerant architectures.

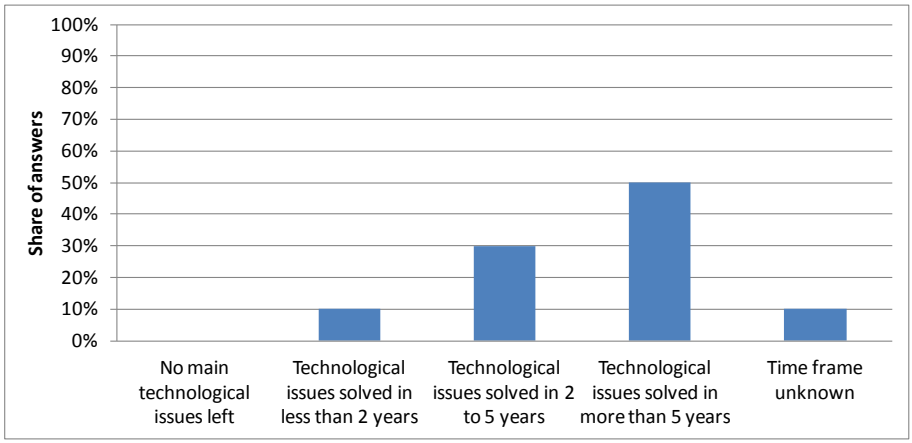
To this aim, the combination of KETs experts' opinions collected through the dedicated survey (whose result is depicted in the below bar chart), the examination of KETs-related patenting activity in respect to this Innovation Field, and desk research activities, have allowed identifying a rather strong interaction of KETs with respect to this Innovation Field, with either fundamental or important contribution mainly by the following KETs:

- Micro- and Nano-Electronics (MNE)
- Photonics (PhT)
- Nanotechnologies (N-T)
- To a lesser extent, Advanced Manufacturing Systems (AMS)



Timing for implementation:

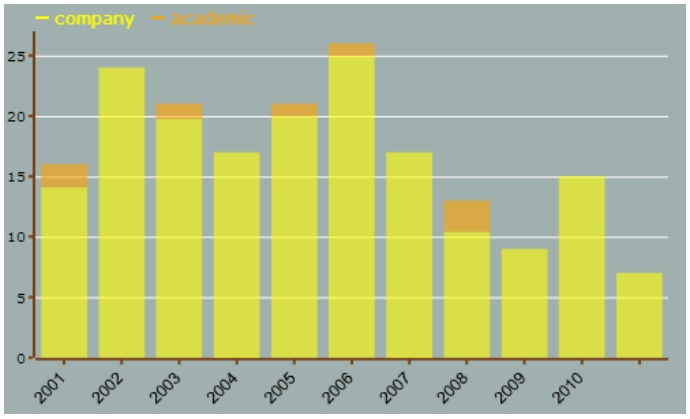
According to the majority of KETs experts' opinions (whose result is depicted in the below bar chart), desk research, and in line with the KETs-related patenting activity in this field, it is considered that the main technological issues holding back the achievement of cross-cutting KETs based products related to this Innovation Field could be solved in a time frame of more than 5 years:



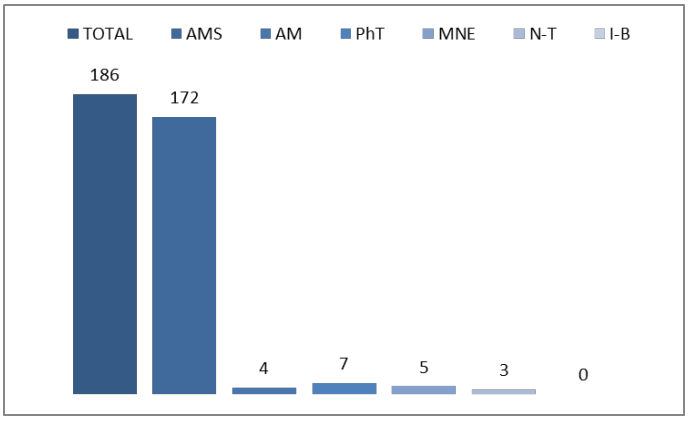
Cyber-security and infrastructure dependability are supported by technology developments but also heavily dependent on non-technical aspects taking time for assembling altogether. Hence, the provision of support in the medium term should be taken into consideration within this framework.

Additional information according to results of assessment:

- ***Impact assessment:***
  - As information-based services take deeper roots into European societies, ensuring reliability and high quality and continuity in the communication services gets more and more crucial. Dependable communication platforms and IT infrastructures are mandatory links for supporting end-to-end communication chain resistance and resilience, protecting citizens' privacy, ensure society's trust in the communication backbone of the inclusive, innovative and reflexive information society.
  - Secure communications will enable fulfilling the Digital Agenda for Europe objectives for citizens to use eGovernment services, as well as supporting the deployment of e-Health/telemedicine, protecting online sales/purchase and e-banking services against malevolent actions and intrusions, ensuring reinforced European protection against unfriendly economic or political intelligence or even cyber war attacks.
  - The European telecommunication systems' industry faces a fierce competition from international competitors, and technological advance in dependability technologies is one of the axes which can comfort its competitiveness.
- ***Results of patents scenario analysis:***
  - 186 exclusively KETs-related patents identified in the period 2001-2011 for the specific Innovation Field
  - Slightly decreasing trend curve (number of patents per year)
  - Highest share of industrial applicants:



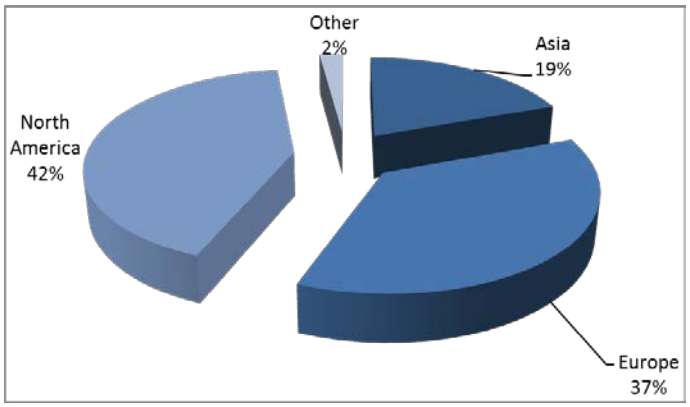
- Patents by KET(s):



- Patents by KET(s) and relevant combinations of KETs:

KET(s)	*Number of patents*
AM	4
AM / MNE	1
AM / N-T	1
AMS	172
AMS / AM	1
AMS / PhT	2
MNE	5
N-T	3
PhT	7

- Patent distribution by (Applicant) organization geographical zone:



- The top applicant positions are shared between European, Japanese and American companies

- Patent distribution by geographical zone of priority protection: