

Dependability Development

DDSI

Support Initiative

DDSI
IST-2000-29202

**R&D Strategy Roadmap
for Information Infrastructure
Dependability**

November 2002

RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)

Project number IST-2000-29202,
supported by
the IST research programme
of the European Community,
managed by
the European Commission DG
Information Society.



DDSI

Report Version: Final

Report Preparation Date: 1 November 2002

Classification: Public

Preparation led by: IABG (D), RAND Europe (NL)

Contract Start Date: 1 June 2001 Duration: 18 months

Project Co-ordinator: RAND Europe (NL)

Partners: RAND Europe (NL); King's College London (UK); Cell Networks (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR); Ernst Basler + Partner (CH), Isdefe (E)

Preface

The dependability of the information infrastructures upon which the Information Society relies is recognised as being of growing importance for European citizens, businesses and governments. The European Council has called for a “comprehensive strategy on security of electronic networks including practical implementing action”¹ and the draft eEurope Action Plan 2005 outlines a range of strategies to promote security practices, a culture of security and trustworthy networks.²

European society is becoming increasingly dependent upon large, complex critical infrastructures which are interconnected in ever more complex ways. The information infrastructure is an ever more significant infrastructure in its own right, as well as being an essential service enabler for other infrastructures. As critical business, social and government processes become more reliant on these computerised information systems and networks, so society becomes more vulnerable to disruptions of these infrastructures as a result of accidental failures, natural disasters or malicious attacks.

Dependability, which has provided solutions in bounded computer-based systems, is the obvious candidate as an integrating concept and approach to addressing the potential misbehaviour of large, computer-based systems of systems. However, current technologies do not seem sufficient to cope with these new challenges. To understand, analyse and manage the risks consequent upon our reliance upon large-scale, complex and interdependent information-based infrastructures requires a major dependability R&D effort.

The inherently transnational nature of these infrastructures and the growing internationalisation of dependencies, threats and vulnerabilities makes this topic an obvious candidate for collaborative action at European level to add value to industry and Member State R&D programmes, leveraging upon the dependability-related scientific and technological effort developed at the national and European levels.

Over the last decade, Europe has organised a substantial programme of dependability R&D that complements national and private sector R&D in dependability and associated areas such as information assurance and security. However, there are a number of drivers for conceiving more effective future European approaches to R&D into dependability, including:

- Increasing dependencies on information infrastructures across all sectors of our society in an environment of growing threats
- Increasing demands by European citizens, society and business for a secure and safe information infrastructure
- Increasing recognition of the cross-cutting challenges posed by information infrastructure dependability; since the risks are borne by all citizens, by business and by states, solutions need to engage all stakeholders
- Increasing recognition of the need to adopt a multi-disciplinary vision of dependability and to draw together different communities to examine information infrastructure dependability from various perspectives
- The emerging European public policy framework for action on dependability and information security/assurance, which requires research support

¹ *Network & Information Security*, Resolution of the European Council, 6 December 2001.

² European Commission, eEurope 2005: Possible Actions

The European Research Area (ERA), a new approach to R&D envisaged by the European Commission, provides the opportunity for a well-conceived and integrated medium term research programme on information infrastructure dependability. Framework Programme 6, the ERA's financial instrument, can be used to support an integrated, multi-disciplinary programme of work that capitalises on European strengths and engages all stakeholders.

This document provides a strategic roadmap for the development of a European R&D programme aimed at improving the dependability of Europe's information infrastructures. The document identifies strategic approaches to be taken to develop a coherent and overarching research strategy addressing all aspects of information infrastructure dependability. It provides a framework for integrating other roadmaps under development dealing with the technological agenda and with requirements in specific areas of dependability and security.

Other Sources

The country inventories upon which the survey of national and international activity was based can be found at www.ddsi.org.

The reports of two R&D Policy workshops (December 2001 and September 2002) can be found at www.ddsi.org.

Acknowledgements

This roadmap could not have been completed without the support and input of experts from the European and international R&D community as well as from industry and government end-users. Our thanks go to all those who participated in the workshops, upon whose writings we drew and who commented on the ideas developed in the course of this work. In particular, Andrea Servida, Maarten Botterman, Luca Simoncini, Marc Wilikens, Brian Randell and Marcelo Masera provided detailed comments on drafts of the document. Responsibility for any mistakes remains with the authors.

Stefano Bruno
Susanne Jantsch
Caroline Mojert
Andrew Rathmell
Christine Schwarz-Hemmert
Lorenzo Valeri

Executive Summary

Vision

A unique opportunity exists for Europe to assure the emerging infrastructures that will support the Knowledge Society, whilst at the same time benefiting European industry. This opportunity can be realised if Europe develops a strategic approach to dependability R&D.

Today, there is a “dependability gap” between the expectations being placed by society upon contemporary information infrastructures and the robustness of these infrastructures. European society is become more dependent upon the large, unbounded, multi-jurisdictional socio-technical systems that constitute the information infrastructure but infrastructure vulnerabilities are legion, ranging from the component level (e.g. “buggy” software) to the societal level (e.g. inadequate legal regimes).

Meanwhile, Europe is moving towards a new infrastructure paradigm, that of an Ambient Intelligent Space. In this environment, intelligence is distributed, pervasive and unobtrusive. New applications such as telemedicine, intelligent roads and personalised e-government will ride upon this infrastructure. Dependable infrastructures are central to this paradigm.

A strategic European approach to R&D must meet the unresolved dependability needs of users operating in the existing infrastructure paradigm *and* “engineer in” dependability to the emerging infrastructures.

A strategic European dependability R&D programme could have the following societal impacts:

- Ensure the achievability of the business, political and social aims of the Knowledge Society vision. The R&D programme must fill the “Dependability Gap.”
- Enable the development of Knowledge Society services by building dependable components and systems of systems.
- Enhance the competitiveness of European industry, notably the software and IT sectors, by enabling them to take the lead in building components for the Ambient Intelligent Space infrastructure, perhaps exploring concepts such as warrantable software.

Dependability as an Approach

Dependability, as a concept that integrates elements such as reliability, safety and security, provides a proven conceptual framework for developing intellectually robust solutions to these challenges. However, attempts to improve dependability are hampered by the fact that information infrastructures have undergone a radical change from the paradigm of centralised control to the *economics of functionality*. Whether one considers the demand for functionality by individual PC users or the reliance by power companies upon the public telecommunications system, it is evident that the traditional approach that pits functionality against dependability is failing to deliver adequately dependable infrastructures to all users.

Therefore, the philosophy of the R&D programme should be to make dependability an integral property of all aspects of the Knowledge Society and to treat it as an enabler rather than as an add on. The functionality-dependability dilemma needs to be replaced by an approach in which dependability is a prerequisite for functionality.

A paradigm shift in dependability is required to address this new environment. A wider range of communities should be embraced so as to develop a truly multi-disciplinary approach to dependability. These communities should be invited to apply their methods to the dependability challenges posed by the system of systems and societal levels. Disciplines and approaches that may be able to contribute include complex systems theory, bio-mimetics (e.g. computational immunology), complex physical systems (e.g. meteorology and oceanography), complex virtual systems (e.g. agent-based systems) and economics.

Research & Policy

In order to fulfil the potential of an enhanced dependability initiative, appropriate research policies need to be developed to derive systematic roadmaps, to optimise research management and to develop effective funding structures as well as to evaluate R&D impacts. R&D policy should embed a continuous process of “envisioning the future,” including drivers, challenges and needs. This will help to systematically categorise and prioritise research requirements.

An important additional function of the European research programme should be to provide analytical support for public policy-making. Currently, the scientific knowledge base upon which policy-makers can base their decisions in the area of dependability is inadequate. A transnational network of experts should be established to develop this knowledge base and to ensure a two-way communication channel with policy makers.

It is increasingly evident that today’s large-scale socio-technical systems can only be assured if the political, social and economic contexts and drivers are understood. The research programme should encompass these environmental factors, for instance the economics of information security.

The Research Agenda

The European dependability research agenda needs to build on existing strengths (e.g. on the component level) but to devote more effort to the system of systems and societal levels. The research programme must address the short-term needs of users of existing systems (“fixing today’s problems”) and lay the foundations for the future infrastructure (“engineering in dependability”).

There are numerous “shopping lists” of possible dependability research topics; the next phase of roadmap activities should systematically categorise and prioritise topics. An initial categorisation could include the following:

- Policy Issues
- Basic Research
 - e.g. Interdependencies; Threats & Risks; Implications of new technologies
- Human Factors
 - e.g. User/Customers; Service Providers & Vendors
- Economic Aspects
- Technical Measures & Capabilities
 - e.g. Protection; Detection; Reaction
- Organisational Measures
- Measurement, Simulation & Testing

Technology Take-up

R&D will only benefit European stakeholders if its results are taken up. At the same time, many user requirements can be met not by long-term research programmes but by exploitation of existing or near to market technologies.

The overarching aim of a dependability initiative in the ERA and FP6 should be to inculcate a *culture of dependability*. To achieve this aim, it will be important to widen the involvement of stakeholders outside existing dependability projects, i.e. the wider research community, national governments, industry, consumers, privacy groups and research policy makers. The research programme therefore needs to include:

- Embedded dialogue between researchers, implementers and users
- Mechanisms for “tactical” research, for instance assisting users with adaptation of existing solutions
- Links between the R&D programme and standardisation bodies
- Support for market mechanisms and awareness activities to stimulate demand for more dependable systems from private and corporate users (e.g. via corporate governance, liability, insurance, legal)
- Education & skills at all levels from young researchers to practitioners, policy-makers and individual users

Contents

Preface 3

Executive Summary 5

1 Background 11

1.1 Infrastructure Dependence and Interdependence11

1.2 Information Infrastructure Dependencies14

1.3 Functionality vs Dependability14

1.4 A Dependability Approach15

1.5 Dependability for the Knowledge Society16

1.6 A European Strategy17

1.6.1 Why Public Investment?..... 17

1.6.2 Why an EU Role? 17

1.6.3 Why an Enhanced IST Dependability Initiative? 18

2 Designing a Strategic R&D Roadmap.....20

2.1 Lessons Learned from Other Roadmap Processes.....20

2.1.1 Roadmap Methods 20

2.1.2 Roadmap Findings..... 20

2.2 The DDSI Roadmap Process21

3 Existing European R&D Capabilities23

3.1 Dependability R&D Issues.....23

3.2 Topics in National Dependability R&D.....23

3.3 European Commission dependability research.....25

3.3.1 Dependability research management..... 26

3.3.2 Major themes of dependability during FP5 26

4 The Roadmap: A European R&D Strategy.....29

4.1 Research policy.....29

4.1.1 Roadmap Processes..... 29

4.1.2 Funding Mechanisms 30

4.1.3 Evaluation 30

4.2 Research Agenda.....31

4.2.1 Research Goals..... 31

4.2.2 Research Topics 31

4.3 Technology Take-up33

4.4 Research & Policy.....33

Appendix 1: R&D Roadmap Development Processes.....35

European Commission FP6 IST Programme35

Working Group on Information Infrastructure Interdependencies & Vulnerabilities36

US Government.....36

UK Government37

Information Assurance Advisory Council38

Appendix 2: National R&D Programmes.....39

Appendix 3: EU IST Dependability Projects.....47

Appendix 4: EU IST Dependability Roadmaps50

Appendix 5: Dependability R&D Topics 51

1 Background

Why do we need a European R&D strategy into information infrastructure dependability?

This section describes the societal challenge posed by our dependence upon critical infrastructures, which are increasingly dependent upon information systems. The section then outlines the need for an EU R&D strategy to develop dependability solutions.

1.1 Infrastructure Dependence and Interdependence

There is nothing new in the observation that society is dependent upon certain infrastructures for provision of services that are critical to the citizen, business and government. Transportation and energy infrastructures for instance, have long been essential to industrialised societies. Other critical infrastructures include finance, government, healthcare, telecommunications and food and water supplies. Societies have long had to deal with these dependencies; infrastructures have been physically disrupted by natural disaster (e.g. floods), accident (e.g. tunnel fires) and malicious acts (war, terrorism). They have also been organisationally disrupted by policies (e.g. Californian electricity market deregulation) or market forces (e.g. collapse of Worldcom & KPNQwest). Societies have deployed a range of measures to manage risks to these infrastructures and to build in resiliency.

The new challenge is posed by the fact that these infrastructures are evolving into what can be termed Large, Complex, Critical Infrastructures (LCCI). The concept of LCCI refers to the fact “that industrialised society could not survive without reliable supplies of energy and good communications” as well as other infrastructures upon which they are interdependent, such as finance and transportation. These infrastructures are “**large** because, while it may be possible to identify individual local or regional networks, they are all interconnected to form national, European and (in the case of communications) global networks.” They are ... “**complex** because each network has to provide a range of services to a wide range of customers and rarely has a single supplier of the services connected to the network.” They are “**critical** because our society would face collapse if any of these infrastructures were unavailable for any extended period of time.”³

Each of these infrastructures can be visualised as a very large system of systems.⁴ Whilst each LCCI system of systems has its own characteristics, in general, contemporary infrastructures can be characterised in terms of the layered model outlined in figure 1. The layers are⁵:

- Physical infrastructures (mainly made up of hardware components)
- Cyber-infrastructures (mainly made up of software components)
- Organisational infrastructures (mainly made up of human operators and by operator supervisory/support systems)

³ <http://www.ist-safeguard.org/>

⁴ Revised version of *DSOS Conceptual Model IC1*, 23 October 2001, <http://www.newcastle.research.ec.org/dsos/deliverables/IC1.pdf>

⁵ Various approaches can be taken to defining infrastructure layers. The model here is adapted from that used in SAFEGUARD to characterise the electrical sector. The addition of the service layer reflects a simple model of communications networks such as the Internet which places “content” as the top of three layers. L. Lessig, *The Future of Ideas* (New York: Random House, 2001), pp. 23-25.

- Strategic Business (service layer)

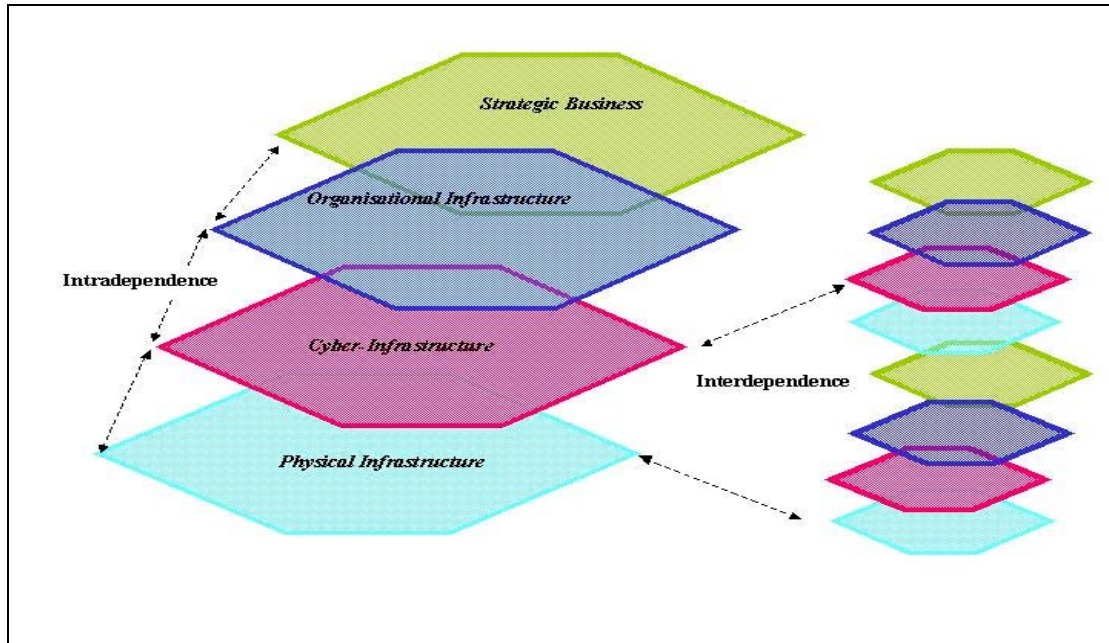


Fig. 1: LCCI Layers⁶

Within each infrastructure, each of these layers is connected to other layers; often these connections will be in the form of intradependencies whereby the state of one layer is dependent upon the state of another layer. There is also a range of connections or linkages between infrastructures. Some of these linkages are relationships of *dependency* whereby the state of one infrastructure influences the state of another infrastructure. Some are also relationships of *interdependency* in which there is a bi-directional influence.

The interdependencies between LCCI have been demonstrated in numerous cases of disruptions to various layers of the infrastructures in developed countries. It has become evident, for instance, that disruptions to the communication infrastructure impact upon the financial system, which in turn may affect the electrical power sector.

However, “identifying, understanding, and analyzing these interdependencies are significant challenges.”⁷ An initial approach is to consider the six dimensions of interdependence sketched in figure 2. These dimensions are: Infrastructure characteristics; state of operation; type of failure; types of interdependencies; coupling and response behaviour; environment.

⁶ Adapted from Safeguard (IST-2001-32685)

⁷ Steven Rinaldi, James P. Peerenboom and Terence Kelly, Complexities in Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies

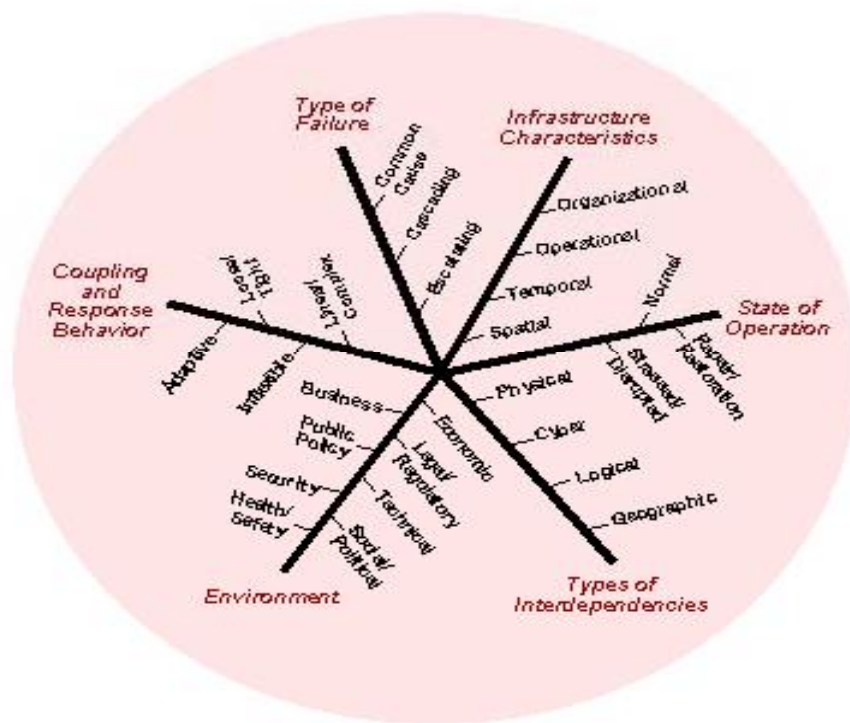


Fig. 2: Dimensions for Describing Infrastructure Interdependencies

Although not yet a model which may be of use to analyse and manage infrastructure behaviour, this approach provides a basis for discussion. Five issues raised by this approach are worth elaborating upon:

- LCCI may display some of the characteristics of Complex Adaptive Systems (CAS), or at least CAS may provide a useful conceptual framework for understanding LCCI
- Interdependencies may be at different layers of an LCCI – e.g. physical, cyber, organizational.
- Interdependencies must also be understood in the broader sense. For instance, the global socio-economic system has an increasing number of tightly coupled dependencies that are not part of any technical system in the narrow context. Examples include financial flows, information flows via the media and patterns of crime and fraud.
- LCCI may be coupled loosely or tightly; the degree of coupling has implications for the type of failure. Tight coupling may lead to cascading failures.
- These infrastructures are socio-technical systems in the broadest sense. They are embedded in, dependent on and influence wider society at many levels. They can only therefore be understood in the context of their environment, which will include factors such as public policy and social perceptions, the economic/market structure, the legal/regulatory framework, health and safety issues, and national security.

1.2 Information Infrastructure Dependencies

The information, or “communications infrastructure,” can be defined as: “the collection of hardware equipment and procedures (software, management) for transporting data needed by an application to deliver specified services to the users.”⁸

Like other LCCI, the information infrastructure can be envisaged in simple terms as having four layers:

- physical (e.g. the wires and computers)
- logical (or cyber) (the software)
- organisational (the people, organisations and processes)
- content and services (both generic intermediate services such as the GRID and sector specific end-user services, applications and communications content)

Today’s information infrastructure is maturing into an era of “pervasive computing,” the implications of which are captured in the European Commission’s concept of “ambient intelligence.”⁹ The future European information infrastructure will involve the convergence of networked embedded and hybrid systems that will immerse citizens in an information environment and in which physical control systems will increasingly migrate online.

Although industrial society has long been dependent upon telecommunications, society’s dependence upon this wider information infrastructure is now becoming more marked, for two reasons.

First, the information infrastructure itself poses increasing difficulties for risk management. Reasons include:

- Reliance upon complex software
- Tight, global coupling
- The fragmentation of governance and ownership of the infrastructure components

Second, other infrastructures are increasingly coming to rely on the information infrastructure for critical business processes (e.g. e-commerce, control communications) and controls of physical systems (e.g. Process Control Systems or SCADA). Other LCCIs are also becoming more dependent on the cyber-layer as they embed computer and software systems into their essential business processes. As highlighted by the Commission in its November 2001 Communication on the e-Economy, information infrastructures and the use of ICT are now central to all business sectors and underpin economic growth and employment.¹⁰

1.3 Functionality vs Dependability

Although dependable software and systems have emerged in particular applications, such as avionics, defence and nuclear power, in general the information infrastructure, notably software components and

⁸ Nicholas Kyriakopoulos and Marc Wilikens, Dependability and Complexity: Exploring Ideas for Studying Open Systems-Full Report, 15 December 2000.

⁹ “Scenarios for Ambient Intelligence in 2010”, report of the Information Society Technologies Advisory Group (ISTAG), <ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf>

¹⁰ Communication from the Commission to Council and the European Parliament, *The Impact of the e-Economy on European Enterprises: Economic Analysis and Policy Implications*, 29 November 2001 COM (2001) 711 Final

the Internet, has not been developed with a focus upon dependability. Instead, the emphasis has been upon functionality. An interdependent combination of factors has been responsible for this: such as lack of application of rigorous software engineering principles, lack of legal liability on software vendors and lack of demand by users. Rather than building in dependability, the market has relied upon vendors to provide *post facto* fixes and on a parallel information security industry to patch holes. On the whole, it has been up to users to integrate components and ensure the dependability of their systems.

It is coming to be understood that this approach will not be acceptable as society becomes even more dependent upon information systems at all levels. User concerns about privacy, digital rights management, legal liability and business assurance, as well as national security concerns expressed by the US Government, are shifting the grounds of the debate. Software vendors have begun to address the problem (e.g. Microsoft's Trustworthiness initiative, Intel's Trusted Computing Platform Alliance and IBM's autonomic computing).

The research challenge will be to develop solutions that will address the economic drivers of suppliers, the affordability of dependability features and society's needs for dependable societal systems.

1.4 A Dependability Approach

Dependability¹¹ has emerged in recent years as an approach to deal with building dependable systems of systems from components and systems; if this approach can be scaled to the global socio-technical systems that constitute the emerging information infrastructure, then we may be able to manage the risks effectively.

Dependability¹² can be defined as “that property of a computer system such that *reliance can justifiably be placed on the service it delivers.*”¹³ Dependability should be seen as: “the ability of a system to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the users.”¹⁴ The dependability of a system is expressed in terms of the following attributes:¹⁵

- **Availability**, involving readiness for use
- **Reliability**, involving service continuity
- **Safety**, involving non-occurrence of *catastrophic consequences* for the environment
- **Confidentiality**, involving non-occurrence of *unauthorised disclosure* of information
- **Integrity**, involving the prevention of *unauthorised modification* or deletion of data
- **Maintainability**, involving the *ability to conduct repairs* and introduce evolutions¹⁶

¹¹ The US concept of Trustworthiness is a similar concept.

¹² See DDSI WP1.1: *Conceptual Framework* for a comprehensive discussion of terminology.

¹³ David Powell and Robert Stroud (Eds), *MAFTIA Conceptual Model and Architecture* (November 20 2001), MAFTIA deliverable D2, p.3. See also the International Federation for Information Processing (IFIP) definition: dependability is “the trustworthiness of a computing system that allows reliance to be justifiably placed on the service it delivers” in J. C. Laprie (ed.), *Dependability: Basic Concepts and Terminology* (New York: Springer-Verlag, 1992), p.4. See also J.C. Laprie, "Dependable Computing and Fault Tolerance: Concept and Terminology", in *Proceedings of the 15 IEEE International Symposium on Fault Tolerant Computing, Ann Harbour, MI, USA, June 1985* (IEEE Press, 1986), pp.2-11

¹⁴ A. Avizienis, J.C. Laprie and Brian Randell, *Fundamental Concepts of Dependability*.

¹⁵ MAFTIA Conceptual Model and Architecture, p. 3. See also: Neil Storey, *Safety-Critical Computer Systems*, (Harlow, UK: Addison-Wesley, 1996).

¹⁶ A. Avizienis, J.C. Laprie and Brian Randell, *Fundamental Concepts of Dependability*, LAAS Technical Report n. 01145, April 2001, p.6

Security encompasses confidentiality, integrity and availability relative to authorised users, as well as accountability, notably authentication and non-repudiation. It is therefore an important element of a dependable system, with particular reference to malicious interference. **Survivability** is a concept that overlaps between dependability and the language of survivability is particularly applicable to open systems operating in hostile environments.¹⁷

1.5 Dependability for the Knowledge Society

The information infrastructures upon which the knowledge society will depend are evolving. The paradigm of an Ambient Intelligent infrastructure involves the following changes from today's information infrastructure:

- from stable to dynamic: technologies, means, stakeholders, links, requirements are evolving continuously
- from complete knowledge to incomplete: what are the structures, functionalities and behaviours of the infrastructure is increasingly more difficult to state
- from bounded to unbounded: all components are connectable, all nodes are reachable from any single point
- from a component-centred view to networked systems: each element matters less, so long as it conforms with standard protocols – services and function emerge from the combination of elements over the network
- from few to many stakeholders: the evolution of services means that any single communication, transaction or computation that uses the information infrastructure engages more and more nodes
- from known connections and interactions to emergent ones: what was a relatively predictable behaviour is becoming opaque for users and service providers
- from clear ownership and responsibilities to diffusion: end-users and services make use of other services on an opportunistic basis, taking ad-hoc advantage of their availability in the on-line world

The changing infrastructures must be matched by a paradigm shift in dependability theory and practice. The new approach to dependability should ensure that:

- all fault types are encompassed; in particular security should be considered as an inseparable dependability attribute
- human and organisational factors are taken into account
- all architectural levels of the infrastructure are considered: components, systems and large scale systems, emergent systems-of-systems, emergent behaviours at the top level infrastructure
- dependability should be engineered into the components and systems
- the design for and assessment of dependability should adapt and evolve as systems evolve

In sum, existing approaches to dependability will not satisfy society's future requirements. The new approach must cope with limited knowledge, ensure that dependability is designed in and is compatible with the increased functionality of the information infrastructure.

¹⁷ Notably, the concepts of “graceful degradation” or “failing soft” are embedded in the notion of survivability.

1.6 A European Strategy

Developing the means to ensure the dependability of our information infrastructures will be a major R&D challenge. Before going into the details of how a European R&D strategy should be shaped, it is worth being clear about three points: the rationale for public investment; the rationale for a multilateral approach; the rationale for an extended dependability initiative within the IST programme.

1.6.1 Why Public Investment?

The rationale for government investment in R&D into infrastructure assurance was made succinctly by the US Government's Critical Infrastructure Protection Interagency Working Group which noted that:

“Despite the fact that the private sector owns and operates the vast majority of the nation's critical infrastructures, it does not invest heavily in long-term, high-risk security-related technologies, especially if they are too easily adopted by competitors, or otherwise unlikely to generate returns that investors can capture. Such technologies are “public goods” – their development and adoption would benefit the nation as a whole, but they would not benefit any single firm enough for that firm to shoulder their investment cost. Therefore, government becomes the only realistic underwriter to ensure that these technologies are developed – a need that extends beyond funding, since these technologies will serve no useful purpose if they are not adopted and deployed.”¹⁸

1.6.2 Why an EU Role?

European citizens increasingly find themselves in an environment in which the information infrastructures upon which they depend transcend national jurisdictions. Whilst it is the primary responsibility of Member State governments to manage risks within their borders, ensuring the dependability of these infrastructures requires European-wide and, indeed, global activities.

The rationale for strategic coordination of R&D at the international level, firstly across the EU and secondly with non-EU partners such as the US, was outlined at a December 2001 EU-US workshop on dependability R&D.¹⁹ Workshop participants concluded that the following were important drivers for international collaboration on R&D in this domain:

- These are international issues that need to be addressed at national and international levels
- Embedded systems are becoming increasingly networked and more complex
- Interdependencies are growing between essential infrastructures
- A shared understanding that global problems require global solutions
- Access to and exploitation of complementary skills & expertise
- Improved cost effectiveness through greater efficiency and faster results
- Improved access to relevant data that is not available nationally

¹⁸ Critical Infrastructure Protection R&D Interagency Working Group, Report On The Federal Agenda In Critical Infrastructure Protection Research And Development, January 2001, p. 9.

¹⁹ EU-US Workshop Report, *R&D Strategy For A Dependable Information Society: Eu-US Collaboration*, 1–2 December 2001, Düsseldorf, Germany, available from www.ddsi.org

An important additional driver for action is that the addition of further members to the EU, all with varying infrastructures and legal regimes, may well introduce further faults into the overall system. Accession provides the ideal opportunity to ensure that these countries add to the overall dependability of the knowledge society and do not detract from it.

1.6.3 Why an Enhanced IST Dependability Initiative?

The policy and programme drivers for an expanded initiative are clear. At the policy level, the eEurope agenda to make Europe a competitive, knowledge-based economy has made clear that the dependability of Europe's information networks is critical to socio-economic success. These needs were emphasised by the Presidency Conclusions of the European Council meeting of 15 and 16 March 2002 in Barcelona, in which the goal of "Connecting European Economies" was clearly expressed, e.g. for the financial markets, for the European energy, transport and communications networks and for quality public services²⁰. This policy statement emphasises the point that it is the interconnection of information networks not just with each other but with other infrastructures that will be the determinant of Europe's future.

The Information Society Technology vision of Ambient Intelligence underpins this policy vision from a programme perspective. The vision puts dependability at the heart of the programme. As the IST Advisory Group (ISTAG) noted in December 2000, one of the essential components of the IST R&D programme that will support the policy objectives should be a:

"Safe and dependable systems initiative: aim to develop reliable/robust/dependable large-scale or complex systems. Will aim to achieve breakthroughs such as self-assembling and self-testing software, component based techniques, hardware that has high levels of redundancy (fault tolerance), support for a massive jump in the requirement for scalability as we move towards ubiquity of computing, building in graceful failure, context based content search tools."²¹

The important conceptual development from the previous IST dependability initiative is the recognition of the need to address dependability in LCCI, i.e. in large, unbounded systems of systems. There is no sole ownership, responsibility or jurisdiction for these systems; new approaches are therefore needed at every stage – from design, through operation to management. Dependability therefore needs to go far beyond the component and system level; the dependability R&D agenda needs to be substantially broadened and enlarged. As the ISTAG noted in June 2002, "security in [the Ambient Intelligent] space will require solutions very different from those in today's systems."²²

The holistic approach towards dependability is reflected in the OECD's concept of "a culture of security." The recently revised OECD Guidelines emphasise that:

"Each participant in information systems and networks is an important actor for ensuring security. Participants should be aware of the relevant security risks and preventive measures, assume responsibility and take steps appropriate to their roles and positions to enhance the security of information systems and networks."

²⁰ see Presidency Conclusions, Barcelona European Council, 15 and 16 March 2002, part I par. 35 – 42, <http://ue.eu.int/newsroom/makeFrame.asp?MAX=&BID=76&DID=69873&LANG=1&File=/pressData/en/ec/69871.pdf&Picture=0>, visited 3 April 2002.

²¹ ISTAG Recommendations for FP6, December 2000

²² IST Advisory Group, Trust, dependability, security and privacy for IST in FP6 (June 2002)

The Guidelines “propose that all participants adopt and promote a culture of security as a way of thinking about, assessing and acting on the operations of information systems and networks.”²³

²³ Guidelines for the Security of Information Systems: Towards a Culture of Security

2 Designing a Strategic R&D Roadmap

How should we go about designing an R&D roadmap?

This section describes the process by which this Roadmap was developed. First of all, the section draws lessons from similar roadmap processes undertaken by other organisations. It then shows how this Roadmap built upon these lessons to achieve its final results.

2.1 Lessons Learned from Other Roadmap Processes

DDSI builds upon R&D road-mapping activities undertaken by the European Commission IST Programme and Joint Research Centre. In addition to these roadmap exercises, DDSI examined analogous R&D roadmap processes from the US Federal Government, the UK Government (Defence Evaluation & Research Agency), the French government (Réseau Nationale de Recherche en Télécommunications) and the Information Assurance Advisory Council (IAAC). Whilst all had slightly different focus, they all considered similar timescales and similar issues. Summaries of the processes can be found in Appendix 1.

2.1.1 Roadmap Methods

All of the methods outlined in Appendix 1 developed some form of roadmap that was based upon an expert assessment of the areas of interest, identified existing capabilities and R&D programmes, mapped these against predicted trends and identified gaps. The main differences between the processes appear to have been:

- The method by which the initial scope was set
- The extent of participation in the process of topic identification, ranging from the narrow DERA approach to the inclusive European Commission and Institute for Information Infrastructure Protection approaches
- The scope of the work (ranging from information security to infrastructure assurance and dependability)
- The degree to which non-technological R&D issues were included
- The degree of structure in the roadmapping process

2.1.2 Roadmap Findings

The findings of these Roadmap processes can be divided into findings on R&D management, participation and findings on R&D topics.

Research Management was examined by the US studies in some detail. One output of the studies was the creation of the Institute for Information Infrastructure Protection (I3P) as an integrating body. The IAAC study also paid attention to questions of research management and funding. IAAC identified the need for more proactive and forward looking R&D management:

“With some honourable exceptions, much of the R&D underway in both the government and corporate sectors, as well as in academia, is not seeking to address over-the-horizon

issues that, given the accelerating pace of change in technology and business practices, are closer than one may think. ...

There are a number of obvious reasons why Information Assurance and Security (IA&S) R&D has remained behind the curve, including the ways in which government R&D plans are formulated and the short-term commercial interests of many private sector sponsors of research.”²⁴

Given these findings, it is important for an R&D strategy to take explicit account of management and structural issues that will determine the utility and effectiveness of publicly funded R&D.

Participation refers both to participation in the roadmap development process and to the involvement of stakeholders in R&D projects. All roadmap processes have recognised the importance of involving a wide range of stakeholders at both stages to ensure that end-user needs are taken into account. The I3P process has been noticeable for its structured, top-down approach to soliciting input from critical infrastructure owners and operators. The European Commission and JRC processes have relied on a bottom up workshop approach to encourage wide participation by stakeholders in both the R&D and the user communities.

R&D Topics identified by the roadmap processes are categorised and summarised in Appendix 5. Comparing findings across roadmaps was complicated by the fact that the processes approached the question from different perspectives and with different ranges of input. In addition, not all of them either prioritised topics or matched needs to timescales.

2.2 The DDSI Roadmap Process

The purpose of the DDSI R&D Roadmap is to provide a strategic and interdisciplinary framework to contextualise the technological R&D Roadmaps being developed to address LCCI and information infrastructure dependability. As well as addressing R&D strategy and policy, this roadmap addresses three specific issues:

- ensure complementarity between national and European R&D
- ensure the international relevance of European R&D
- widen the stakeholder base for an involvement in future dependability R&D programmes

This Roadmap has used a forecasting approach - extrapolating current trends and identifying solutions to meet desired end-states.²⁵ The Roadmap process, outlined in Figure 1, included the following steps:

- i) Identifying the need for a European R&D strategy by:
 - a. Examining the information infrastructure dependability challenges
 - b. Examining the policy & programme drivers
- ii) Drawing lessons from previous and parallel R&D roadmap processes
- iii) Undertaking a state of the art overview using analyses of national and international R&D activities to generate baseline data on current R&D initiatives and management structures

²⁴ *R&D for CIP*, IAAC Seminar Report, November 2000, available at www.iaac.org.uk.

²⁵ Although the roadmap took as a starting point the scenarios used by ISTAG, it has not used scenario-based back-casting techniques.

- iv) Convening an EU-US expert workshop to identify consensus amongst technologists and R&D programme managers about priorities
- v) Drafting a background paper synthesising the findings of stages i to iv.
- vi) A cross project workshop with European technology experts, research managers and industry end-users

The benefits of this forecasting and consultative approach were that it derived a robust Roadmap and developed a commonly owned and agreed body of knowledge amongst a cross-sectoral group of stakeholders. The common ownership of this knowledge was an important output since it is hoped that stakeholders will base their more detailed roadmaps on this common vision.

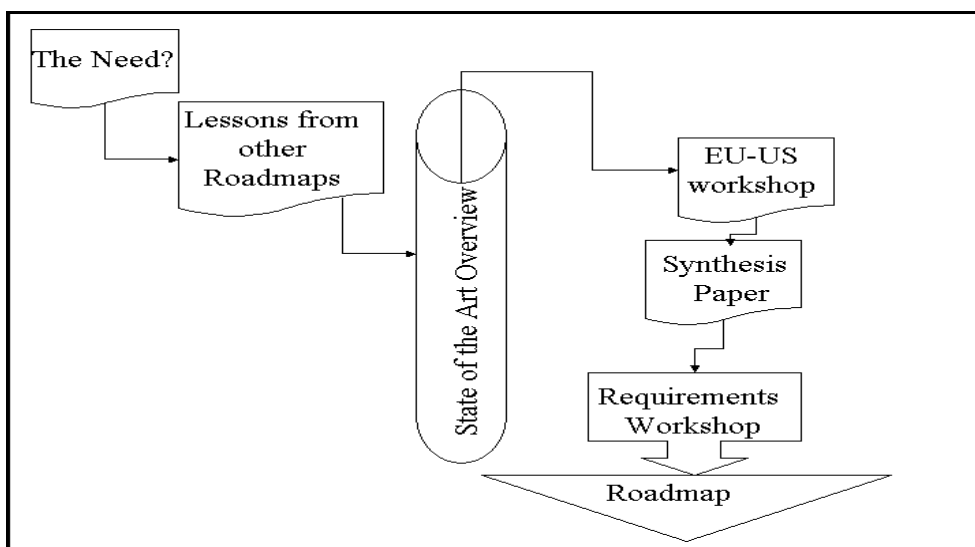


Fig. 3: Roadmap Process

3 Existing European R&D Capabilities

Where are we now in information infrastructure dependability research?

This section provides an overview of information infrastructure dependability related R&D activities in Europe. This section draws on the comprehensive material prepared during the country surveys and summarised in appendices 2 and 3.

3.1 Dependability R&D Issues

Currently, information infrastructure dependability related R&D is not at the top of the R&D agenda of European countries. R&D in this field is scattered and non-existent in some countries. This is reflective of a general lack of a co-ordinated approach towards information infrastructure dependability R&D.

There are centres of excellence in Europe for dependability R&D and related issues such as security, trust and confidence. However, most R&D organisations focus their activities on one specific aspect of dependability or, more usually, information security (e.g. virus research, fault tolerance, vulnerability and threat analysis, risk management, intrusion detection, cryptography, PKI, digital signature, payment assurance, etc.). Holistic and multidisciplinary approaches including several issues are beginning to be encouraged in national research programmes but they are not common.

In addition to the lack of coordination and multidisciplinary, dependability R&D tends to be linked most closely to its “traditional” user base, including defence and transportation. There is limited linkage to new industry sectors.

3.2 Topics in National Dependability R&D

A number of initiatives have examined European strengths and weaknesses in specific areas of R&D. The French Government’s Key Technologies Programme measures Europe’s position in both scientific/technical (R&D) and industrial/commercial strengths. In relation to “trust and confidence enabling tools,” the 2000 report rates Europe’s scientific and technical level as medium and its industrial and commercial position as weak.²⁶

Building on such surveys and the Country Status Report prepared by DDSI, this sub-section summarises the main strengths of European dependability related R&D.²⁷ The overview shows R&D being conducted across a broad variety of topics. To get a better general picture, these themes were classified into seven main R&D areas. The areas and their relative importance in European R&D efforts are shown in the figure below.²⁸

²⁶ Rapport Technologies-Clés 2005. Ministère de l’économie et de l’industrie. Paris, 2000.

²⁷ The information is mainly based on the survey conducted for the preparation of the DDSI WP 2 report “Status and Directions of National Dependability Policy Environments”, August 2002.

²⁸ Relative importance has been estimated taking into account the frequency of the nominations of the main R&D areas in the DDSI WP 2 report “Status and Directions of National Dependability Policy Environments”, August 2002. It is important to note that due to limitations on the information gathered, this can only be an approximate evaluation.

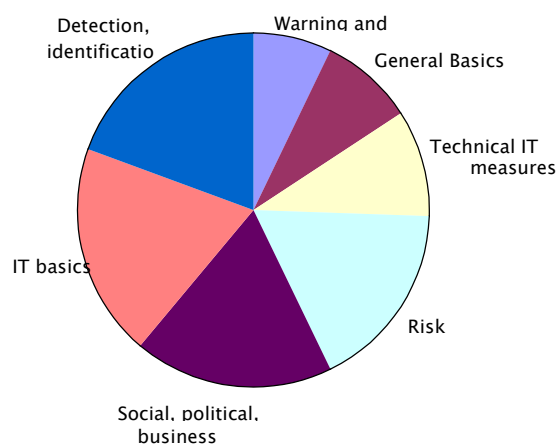


Fig. 4: Main Dependability Related R&D Areas in Europe²⁹

The main R&D areas include the following R&D issues:

Main R&D areas	Dependability R&D issues
General Basics	<ul style="list-style-type: none"> • Verification (tools) • Fault tolerance • Reliability of systems • Survivability of systems
IT basics	<ul style="list-style-type: none"> • Virus research • Secure systems architecture • Access control • Secure data transmission • IP networks security • Data protection • Security systems integration
Risk Management	<ul style="list-style-type: none"> • Vulne mitigation
Warning and alert	<ul style="list-style-type: none"> • Information and network assurance/ security • Warning and information sharing • Early warning models

²⁹ Source: DDSI WP 2 report “Status and Directions of National Dependability Policy Environments”, August 2002.

Main R&D areas	Dependability R&D issues
Technical IT security measures	<ul style="list-style-type: none"> • Intrusion detection • Failure/fraud detection • Monitoring and detection
Detection, identification	<ul style="list-style-type: none"> • Cryptography • Secret sharing protocols • (Pseudo) Primality • PKI • Digital signature • Watermarking • Secure channel coding
Social, political, legal, business aspects	<ul style="list-style-type: none"> • Social, political and legal aspects • e-commerce • Payment assurance • Mobile communication • e-voting • Multimedia and communication

Significant efforts seem to be underway in the areas of detection/identification, IT basic research, risk management, and in business, social, political, and legal aspects. However, social, political, and legal aspects of dependability are in the early stages of basic research. A more detailed analysis shows cryptography, vulnerability analysis and anti virus research to be the most thoroughly examined R&D issues.

Non-European countries like Australia have put a strong emphasis on cryptography and intrusion detection as well. Japan focuses its R&D efforts on four main areas: key technologies for network security, highly-reliable back-up systems, network failure detection, and unauthorised access tracing. In the USA the focus is on vulnerability and threat analysis, risk assessment, system protection and information assurance, reconstruction of damaged or compromised systems, as well as intrusion detection.³⁰

3.3 European Commission dependability research

In the course of FP5, dependability attracted increasing attention as more stakeholders became aware of their growing dependence upon information infrastructures.³¹ In 1997, an initiative was launched as part of the RTD Information Technologies Programme to examine novel dependability issues related to Europe’s information society. It became evident that a comprehensive consultation process was needed to capture the multi-dimensional and multi-actor structure of dependability R&D challenges. A number of

³⁰ <http://www.ciao.gov>.

³¹ See: <http://deppy.jrc.it>

meetings and workshops were organised to both consolidate the community and to enlarge it by engaging industry, governments and users.

These efforts led to the European Dependability Initiative, whose primary objective was to foster trust and confidence in network and information systems through dependability-enabling technologies. From the outset, the Dependability (DEPPY) initiative appreciated the fact that information infrastructures did not recognise national or regional boundaries. An international approach was required. This was especially true in the R&D domain where the sharing of information was necessary to avoid duplication of efforts.

DEPPY's international perspective was evidenced in workshops and exchanges between European and US academics, research management and industry officials with an interest in dependability-related issues.³² Coming under the EU-US Science & Technology agreement, this collaboration has paved the way for more integrated international approaches in the future.

3.3.1 Dependability research management

The content of the FP5 dependability work programmes was derived from various sources:

- consultation via workshops and constituency building exercises with technologists, especially European dependability R&D community
- consultation with infrastructure owners, operators and users via workshops and seminars
- European Council policy initiatives (e.g. eEurope 2002)
- dialogue with US R&D agencies
- responses to calls for proposals

3.3.2 Major themes of dependability during FP5

The FP5 programme's strategic agenda comprised three elements.³³ First, funding was directed towards fundamental research activities aiming at:

- a) understanding and managing vulnerabilities of complex and large scale information infrastructures
- b) mastering information assurance, especially in relation to increasingly ubiquitous and scalable computing environments
- c) assessing the role of information as a critical asset for the competitiveness of business

Second, the Commission provided financial support for industrial and pilot research projects. In these cases, particular attention was given to the identification of specific technological gaps. Third, there was a commitment to foster both collaboration and information sharing among European researchers and with non-European institutions. Particular attention was directed towards the exchange of best practices and technical knowledge.

This agenda was reflected in the contents of the IST programme:

³² Reports of these US-EU workshops are available at: <http://deppy.jrc.it/>

³³ For an overview of dependability-related projects carried out during FP4, see Andrea Servida and Tom Jackson, European Dependability Initiative: Inventory of EC Funded Projects in the Area of Dependability, Report prepared by the Joint Research Centre under the sponsorship of the European Commission Information Society Technologies Programme, January 2000 available at <http://deppy.jrc.it>

- In 1999, the IST programme focused primarily on analysis of the dependability of services and technologies in the context of ubiquitous, complex and scalable large-scale infrastructures.
- In 2000, attention was directed towards the promotion of co-financed industry research projects, which continued to look at areas indicated the previous year, as well as fields like dependability of networked embedded systems, information assurance, and survivable systems.
- In 2001, the Commission decided that it was necessary to examine potential innovative and multi-disciplinary approaches to dependability, risk management methodologies and behaviours. Particular focus was also directed towards consolidating international collaboration.
- In 2002, the IST was coming to a close. The last call was targeted primarily to develop detailed R&D roadmaps in specific areas.

The figure below provides a matrix that maps the areas of R&D supported in FP5 against their application to specific infrastructures.

	General relevance	Transport	Telecoms	Electrical Power	e-commerce
Fault tolerance	MAFTIA, FIT, AMATISTA				MAFTIA
Embedded systems	DSOS, DEPAUDE	SAFEAIR			
Software engineering	MATISSE				CASENET
Measurement	DBENCH				
Risk Analysis	CORAS				DRIVE
Web security	HARP				
Survivability			CAUTION, SAFEGUARD	EXAMINE, SAFEGUARD	
Organisational	CABERNET				
Policy	DDSI				

Fig. 5: FP5 Information Infrastructure Dependability R&D

4 The Roadmap: A European R&D Strategy

What should the R&D Roadmap address?

A strategic European approach to R&D must meet the unresolved dependability needs of users operating in the existing infrastructure paradigm *and* “engineer in” dependability to the emerging infrastructures.

A strategic European dependability R&D programme could have the following societal impacts:

- Ensure the achievability of the business, political and social aims of the Knowledge Society vision. The R&D programme must fill the “Dependability Gap.”
- Enable the development of Knowledge Society services by building dependable components and systems of systems.
- Enhance the competitiveness of European industry, notably the software and IT sectors, by enabling them to take the lead in building components for the Ambient Intelligent Space infrastructure, perhaps exploring concepts such as warrantable software.

A Research & Development strategy must include the following components:

- R&D Policy
- R&D Agenda
- Technology Take-up
- Research for Policy Support

4.1 Research policy

In order to fulfil the potential of an enhanced dependability initiative, appropriate research policies need to be developed to derive systematic roadmaps, to optimise research management and to develop effective funding structures as well as to evaluate R&D impacts. R&D policy should embed a continuous process of “envisioning the future,” including drivers, challenges and needs. This will help to systematically categorise and prioritise research requirements.

Research policy needs to address the following components: roadmap processes; management structures & funding mechanisms; evaluation.

4.1.1 Roadmap Processes

The EU process for developing technological roadmaps, i.e. the content of the research programme and the prioritisation of topics, has been described in section 2. The call 8 roadmap projects will populate the technological R&D agenda; AMSD will integrate the roadmaps. It is however vital that the roadmap process be an ongoing one that:

- Captures the range of technological, social, economic and policy drivers that will require EU-wide R&D out to 2010
- Engages stakeholders to ensure that the research agenda has wide buy-in

- Widens the R&D agenda to ensure a multi and interdisciplinary approach that addresses the future needs of citizens and businesses
- This requirement can be met by adopting the recommendation of the IST Advisory Group that a “specific advisory group should be established so as to facilitate a dialogue between the parties affected by security concerns.”³⁴

4.1.2 Funding Mechanisms

FP6 aims to establish a more agile structure to manage European research projects.³⁵ New funding instruments will aim to both strengthen the European Research Area and to cater for the increasingly complex needs of Europe’s information society. These instruments are summarised below.

FP6 R&D Management Instruments

FP6 instruments will include both new instruments (*integrated projects and networks of excellence*) and traditional instruments (stairways of excellence and specific support actions).

Integrated projects aim to establish a critical mass of activities and resources to achieve ambitious but clearly defined scientific aims. Their strategic goal is to increase Europe’s competitiveness and meet social needs.

Networks of excellence aim to both strengthen Europe’s research excellence in specific areas through networking activities and to develop new knowledge and expertise.

Article 169 refers to Commission’s initiatives supporting national research programmes.

Stairway to excellence/specific targeted research projects refer to initiatives primarily aimed at fostering the transition from FP5 to FP6. These are expected to be similar to cost-sharing and coordination instruments implemented within the FP5 Programme. The use of these instruments is expected to progressively disappear as FP6 proceeds.

Fig. 6: FP 6 Management Instruments

The funding mechanisms need to ensure an appropriate balance between applied and fundamental research; industry support can be expected for applied research but less so for fundamental research.

4.1.3 Evaluation

Any R&D programme should have embedded within it an evaluation process to measure its effectiveness against pre-planned measures. An R&D strategy should explicitly incorporate an evaluation strategy from the outset. Effectiveness assessment is increasingly becoming a standard in R&D programmes.

One approach may be a simple input/output logic model describing the funding-to-use process. This would include 5 stages: Needs assessment; Inputs; Process; Outputs; and Outcomes. Each of these stages would be assessed using PESTLE (Political, Economic, Social, Technological, Legal, Environmental) analysis. The analysis could be undertaken for a number of stakeholders, such as the European Commission, research consortia, industry end-users and citizen representatives.

³⁴ IST Advisory Group, Trust, dependability, security and privacy for IST in FP6 (June 2002)

³⁵ For update of developments related to FP6, see <http://www.cordis.lu/fp6/>

4.2 Research Agenda

The philosophy of the R&D programme should be to make dependability an integral property of all aspects of the Knowledge Society and to treat it as an enabler rather than as an add on. The functionality-dependability dilemma needs to be replaced by an approach in which dependability is a prerequisite for functionality.

A paradigm shift in dependability is required to address this new environment. A wider range of communities should be embraced so as to develop a truly multi-disciplinary approach to dependability. These communities should be invited to apply their methods to the dependability challenges posed by the system of systems and societal levels. Disciplines and approaches that may be able to contribute include complex systems theory, bio-mimetics (e.g. computational immunology), complex physical systems (e.g. meteorology and oceanography), complex virtual systems (e.g. agent-based systems) and economics.

4.2.1 Research Goals

A future European dependability R&D programme needs the following features:

- It should consider the period to 2010, considering FP6 as a step towards longer range goals
- It should be clearly explainable to policy-makers and users outside the research community
- It should be interdisciplinary
- It should have short, medium and long terms foci
- It should combine both applied and fundamental research

An important goal should be to situate European R&D in a global context. The European research programme should identify areas of synergy and avoid duplication between Europe and its major partners, notably the USA. This will pave the way for a truly integrated international response to this challenge.

4.2.2 Research Topics

The precise content of the FP6 R&D programme will be determined by the results of the current roadmapping exercise but there remains a tremendous challenge to capture, map and prioritise research needs into information infrastructure dependability. The review of ongoing R&D presented in section 3 and the roadmaps reviewed in section 2.1 demonstrate the scale of the challenge. The technological roadmap will have to organise and prioritise the topics of interest; this will involve integrating many disciplinary perspectives as well as capturing user requirements.

A welcome step in the process of defining a coherent R&D agenda would be to develop a consensus set of categories for R&D topics. The Internal Reflection Group document of June 2002 provides a useful starting point but more work will be required to achieve convergence between disciplinary perspectives. Based upon the work surveyed for this Roadmap and consultations undertaken at DDSI workshops, the following categories of topics, with some specific examples highlighted.

- > Policy Issues
- > Basic Research
 - * Interdependencies
 - * Threats & Risks
 - * Security implications of technological developments
- > The Human Factor
 - * Users/Customers
 - * Service Providers and Vendors
 - * Other
- > Economic Aspects
- > Technical/Technological Measures & Capabilities
 - * Protection
 - * Detection
 - * Reaction
 - * Other
- > Organisational Measures
- > Measurement, Simulation & Testing

Fig 7 R&D Topics in information infrastructure dependability

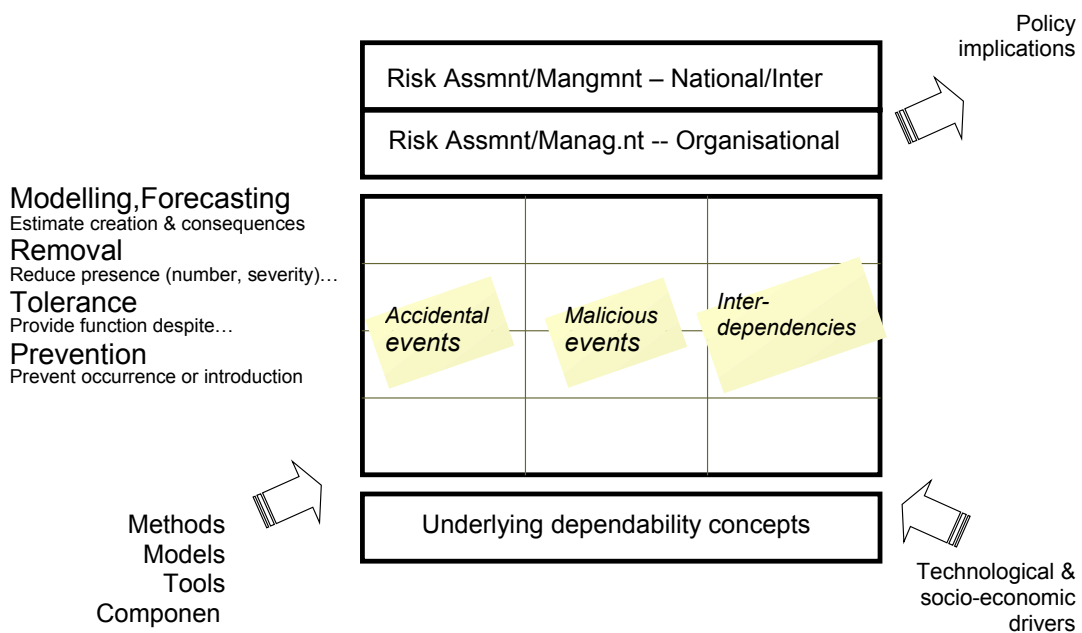


Fig 8: A Dependability Model for Categorising Research Requirements

4.3 Technology Take-up

R&D will only benefit European stakeholders if its results are taken up. At the same time, many user requirements can be met not by long term research programmes but by exploitation of existing or near to market technologies. A central feature of the European research programme, therefore, must be to build in mechanisms for meeting user needs and ensuring technology take-up. Three mechanisms need to be included:

- education and training
- technology transfer
- standards, best practices and guidelines

Whilst public and user awareness of dependability remains limited, there is evidence that awareness is increasing as cyber-abuse escalates. More importantly, as we move into an era of pervasive computing and applications upon which all individuals and businesses will depend, such as health care and e-government, it is likely that user awareness will increase. Already, privacy concerns in relation to government databases and patient records are prompting debate over information security in many European societies.

The R&D programme can build on this trend by focusing both upon the education of individuals before they enter industry *and* on the direct transfer of knowledge to industry. Education should be at all levels – from general awareness and ethical education at school to specialised post-graduate education. Post-graduate education should adopt the multi-disciplinary approach to dependability recommended above. Specialised education also needs to formalise implicit knowledge. For instance, most security architecture design is undertaken by specialists who have gained “hands-on” experience. This knowledge needs to be codified and formalised so it can be passed onto future generations of students.

Technology transfer should place a greater emphasis on sharing best practices and through the creation of guidelines and standards. Methods such as case studies, pilot projects and industry-academic exchanges will help optimise the application of existing knowledge and best practices.

In addition, the research community needs to develop adaptive processes to help users (in the private and public sectors) meet their “tactical” research needs. Whilst not detracting from long-term research, such tactical research will be critical to meet user needs and to ensure existing research is pulled through and supported by the ultimate beneficiaries. Such information sharing initiatives should ideally lead to the development of tools that can be applied across different environments and situations.

4.4 Research & Policy

FP6 calls for research that provides analytical support for public policy-making. Such research is nowhere more needed than in relation to dependability. Currently, the scientific knowledge base upon which policy-makers can base their decisions in the area of dependability is inadequate. As the knowledge society develops and IST applications become pervasive, individual and corporate users will require ever more actions from policy-makers. Already, policy-makers are struggling to deal with topics in which inadequate scientific knowledge along with disagreement about ethical values are complicating policy-making, for instance in relation to cyber-crime or privacy.

Therefore, Europe needs to develop mechanisms for the intensive two-way communication of requirements and problems between the R&D community and policy makers, and an increased awareness

of such communications needs on both sides. Established mechanisms for multi-actor dialogue such as workshops and international policy and business fora will be important but these will need to be supplemented by new fora that bring together researchers from many disciplines, policy-makers and business and civil society representatives. Practical steps could include:

- A transnational network of experts to develop this knowledge base and to ensure a two-way communication channel with policy makers.
- Demonstration platforms in which stakeholders can explore the implications of new technologies and applications and in which multi-actor scenarios can be used to elicit views, identify differences and options and generate consensus. The embryonic EU Cyber-crime Forum provides a useful case study for such platforms.

Appendix 1: R&D Roadmap Development Processes

Strategic roadmaps for information infrastructure dependability R&D have been, or are being, developed by a number of bodies. By reviewing prominent examples, lessons can be learned for the development of an overarching EU R&D roadmap process.

For the sake of comparison, DDSI examined five examples: the overall FP6 IST roadmap process; the Joint Research Centre's Working Group on Information Infrastructure Interdependencies & Vulnerabilities; the US Federal Government; the UK's Defence Evaluation & Research Agency; and the Information Assurance Advisory Council. These are by no means exhaustive of efforts to roadmap R&D needs in this area but their methods, and findings provide useful lessons for the EU process.

European Commission FP6 IST Programme

The overarching direction of R&D in FP6 is set by the policy and IST programme framework. This includes the Ambient Intelligence vision developed by the IST Advisory Group using scenario techniques and the eEurope policy agenda.

Three main methods have been used to help the Commission's Internal Reflection Group to inform the exact content of the work programme. First, a number of workshops were held with technologists, end-users and other stakeholders. Prominent examples included an EU-US workshop held in Düsseldorf in December 2001 and a workshop hosted by LAAS in Toulouse, also in December 2001.

Second, in November 2001, the IST Programme issued its eighth and final call for proposals. A number of dependability-related roadmap projects have since begun work³⁶ These roadmaps are expected to "set strategic goals relevant at the European policy decision-making level".³⁷ The topics selected include:

- Integrated approaches to dependability and policy development
- Embedded systems
- Critical infrastructure modelling & simulation
- Privacy & Identity Management
- e-commerce & mobile security
- Biometrics
- Smart cards
- Cryptography

Third, on 30 May 2002, the European Commission organised an open workshop to allow stakeholders to present proposals for research areas in the fields of trust and confidence to be addressed by FP6. These were used to inform a report issued in June 2002.³⁸ This report points to the following six areas of R&D interest in the context of trust and confidence:

³⁶ Information about FP6 is taken from <http://www.cordis.lu/rtd2002/fp-activities/activities.htm>

³⁷ Andrea Servida and Marcelo Masera, "Workshop on Dependability in Information Society: Future Scenarios and R&D Challenges, LAAS-CNRS, Toulouse, 12-14 December 2001 available at <http://deppy.jrc.it>

³⁸ European Commission, "Trust and Security-Contributions from the FP6 Internal Reflection Group" Draft Version 3.0 12/06/2002 available at <ftp://ftp.cordis.lu/pub/ist/docs/irg-tc-v3.pdf>

- securing the infrastructure
- dependability and interdependencies
- managing identity
- mobile security
- securing digital assets
- new computing architectures and web services

In addition, the report emphasises the need to build wider constituencies as a central element in Europe's search for dependable information infrastructures. These constituencies include:

- a) infrastructure operators (telecommunications, energy, transportation, etc...)
- b) manufacturers
- c) research and academia
- d) public administration and government bodies

Working Group on Information Infrastructure Interdependencies & Vulnerabilities

The Working Group on Information Infrastructure Interdependencies & Vulnerabilities (I3V) was launched in 2001 by the Joint Research Centre as part of its institutional support for DG Infso. The aim of the WG was to bring together researchers and end-users from different infrastructures to identify the priority topics for R&D at European level. The Group was designed to provide support for preparation of the FP6 research programme both by identifying topics and by building communities of interest.

The WG held a number of workshops that succeeded in assembling communities of interest, primarily drawn from the ICT, energy, telecommunications and healthcare infrastructures and R&D communities. Workshops held in the spring of 2002 resulted in initial roadmaps for sector-specific R&D, which were reflected in a number of workshop reports.

US Government

The US federal government initiated a strategic approach to roadmapping R&D requirements for CIP, including cyber-security³⁹ in 1998. The National Science and Technology Council established an Interagency Working Group that drew upon the work of 20 federal departments and outside advisers. The Working Group produced a number of reports – “Blue Books” – that outlined federal R&D priorities in the short, medium and long term. These roadmaps became the basis for successive federal budget investments in R&D.

One of the recommendations of the Working Group was the establishment of an Institute for Information Infrastructure Protection (I3P) as a new way of managing and coordinating the national R&D effort. In the course of 2002, the Institute for Security Technology Studies, along with RAND and Mitre, has been undertaking a roadmap process to develop a national cyber-security R&D agenda. The iterative process adopted by the I3P is indicated below in Figure 3. Important elements of the process are the development of mechanisms to validate and revise the R&D agenda and the focus upon wide community

³⁹ Analogous to information infrastructure dependability

involvement. Rather than relying on a relatively small group of technologists, the I3P is undertaking a formal consultation process to gather input from the full spectrum of stakeholders, including representatives of critical infrastructure domains, industry solution providers and government.

It is important to note that this process has been supported by private sector efforts in the context of the National Plan to define sector-specific R&D needs for critical infrastructure sectors. These efforts have been facilitated by the Critical Infrastructure Assurance Office and by leading industry players such as Cisco Systems.

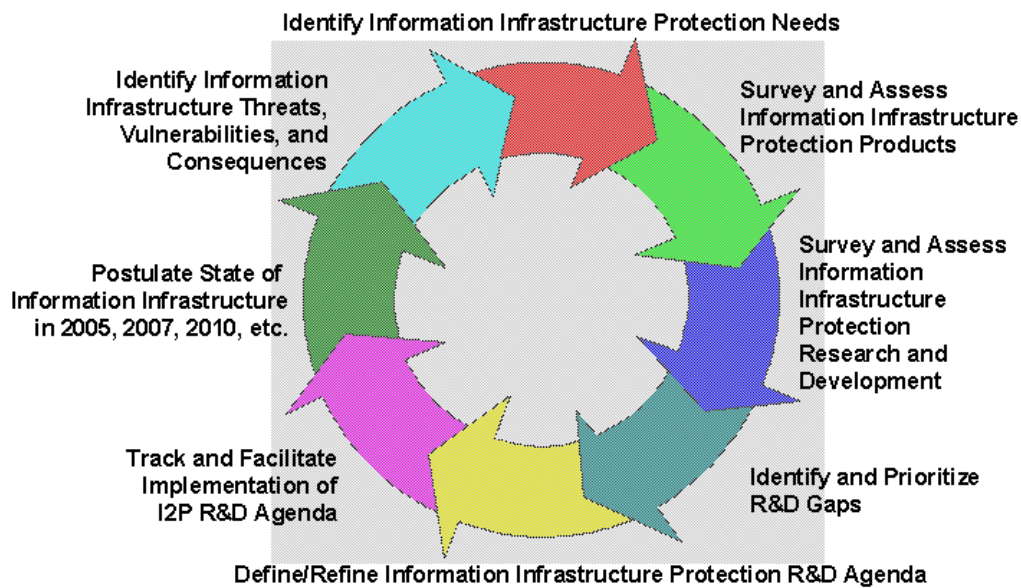


Fig. 7: The I3P R&D Agenda Definition Process

UK Government

In 2000, the UK’s Defence Evaluation Research Agency (DERA) undertook a review of national information security R&D needs on behalf of central government. The method chosen was for the government committee overseeing the work to define the areas of interest by arriving at a “top ten” list of information security R&D issues. Reports were then commissioned from within government, from academia and from industry to determine the state of the art in each issue, to identify national strengths and to predict future developments.

The study was intended solely as a summary baseline but its authors concluded that the selection of the top ten information security priorities was valid. UK strengths were recognised but so was the potential for collaboration, for instance with the USA and European partners, in areas that were not prioritised in the UK list. A particular gap in the original list was in the extension of R&D topics from information security to the wider domain of Critical Infrastructure Assurance.⁴⁰

⁴⁰ A summary of the study is available from www.iaac.org.uk

Information Assurance Advisory Council

In 2000 and 2001, the Information Assurance Advisory Council (IAAC) convened a government-industry Working Group to examine the “factors due to the evolution of technology based capabilities that should guide the establishment of coherent Information Assurance and Security (IA&S) R&D policies.”⁴¹ The Working Group consisted of IAAC members and invited participants, drawn from government, technology developers and users. The group used a combination of research, consultation and formal roadmapping to identify the technology, policy and risk drivers and to derive a time-based roadmap of future R&D requirements.

The formal roadmapping exercise was underpinned by the scoping research and analysis of R&D roadmaps outside the UK. It began with a knowledge capture session from the cross-sectoral participants who were directed to consider developments out to 2010. The knowledge was then structured against a timeline to identify the key drivers and turning points that should shape an R&D strategy.⁴²

⁴¹ IAAC R&D Working Group, Policy Paper summary at www.iaac.org.uk

⁴² The results and roadmap diagram are available at: www.iaac.org.uk.

Appendix 2: National R&D Programmes

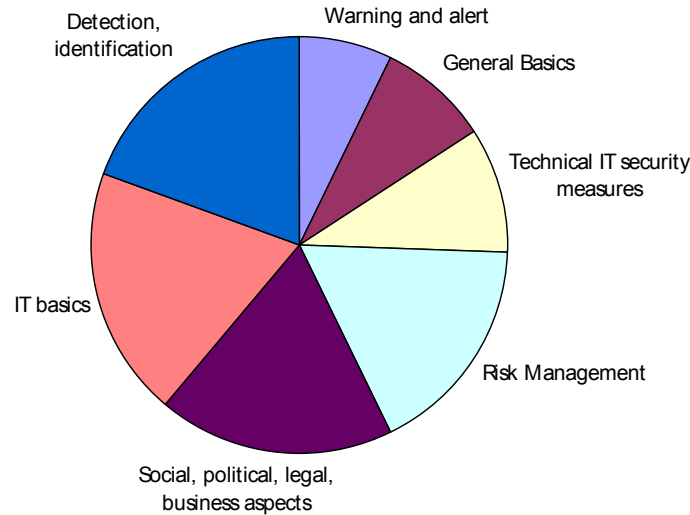


Fig. 8: Main Dependability Related R&D Areas in Europe⁴³

The following tables provide overviews of R&D management processes, programmes and topics in European and non European countries. The information is based on the DDSI WP 2 report “Status and Directions of National Dependability Policy Environments”, August 2002. The gaps are due to non-existent efforts in the respective country or due to a lack of easily available information.

Tab. 1: European Member State R&D Management Processes

Country	Leading R&D organisations	Main funding source ⁴⁴	Approaches
Austria	K _{plus} (competence centres); mainly universities	g, b	
Belgium	Independent organisations (private research and universities)		2 parallel approaches
Cyprus	Government	g	Dependability related R&D almost non existent, lack of coordinated and central approach
Czech Republic	Universities, government offices, private sector		

⁴³ Source: DDSI WP 2 report “Status and Directions of National Dependability Policy Environments”, August 2002.

⁴⁴ g = government; b = business

Country	Leading R&D organisations	Main funding source ⁴⁴	Approaches
Denmark	Danish Technological Institute (DTI): private, non profit company (acts as an interface between industry, government, research community) Aalborg university		
Finland			
France	LAAS (Laboratory for Analysis and Architecture of Systems) RNRT		LAAS: cooperation approach -> has developed 30 co-operation agreements with 15 countries
Germany	Universities	Complex situation	Several
Greece	Universities	g	
Hungary	Government		
Ireland	Some academic departments		Dependability related R&D almost non existent; just at the beginning
Italy	Government supported centres; industry is becoming more interested CNUCE Institute (government supported) ENEA (government supported) CESI centre Telecom Italia Lab		Dependability related R&D is not a strong priority in Italy so far
Liechtenstein			
Luxembourg			
Netherlands	TNO-FEL TELIN (builds a bridge between the government and companies) GigaPort (initiative by several ministries)		
Norway	Above all public sector: Norwegian Defence Research Establishment Academic institutions		So far only few activities

Country	Leading R&D organisations	Main funding source ⁴⁴	Approaches
Poland	Academic departments (universities)		Special situation: PL R&D priorities are very much geared towards economic growth. PL needs to use its R&D capability to take advantage of the fact that it is seen as an entry point for Eastern Europe markets. Scientific technology transfer between academia and industry is viewed as an essential part of R&D process. State expenditure will be increased in this area. An award system of prizes will be implemented for the most innovative products.
Portugal	Mainly universities		
Spain	Spanish Council for Scientific Research (CSIC), some universities		CSIC collaborates with other national, regional, and local administrations, other research organisations, universities, and private corporations (nationally and internationally)
Sweden	Universities, agencies EnerSearch AB (industrial research consortium) FOI		Academic institutions are not only looking at dependability from a technological perspective. There is increased interest in the socio-political and economic implications. This includes also industry and civil society as a whole
Switzerland	Mainly academia		
United Kingdom	Most important at Government level: DSTL, QinetiQ (formerly DERA; now privatised) Several universities Private sector (IBM, Hewlett Packard, etc.) Think tanks on social aspects (FIPR, STATEWATCH, Privacy International)	g, b	Research Councils have sought to consolidate dependability research through the DIRC (Interdisciplinary Research Collaboration on Dependability of Computer-Based Systems)

Tab. 2: Overview of R&D programmes and issues in European countries

Country	Main programmes	Main R&D issues
Austria	FIT-IT (dealing with embedded systems, currently being developed)	Vulnerability and threat analysis, cryptography, access control (main strengths)
Belgium	IWT (Institute for the Promotion of Scientific/Technical Research in Industry) plays an important role in EU R&D programmes, most notably in the European Union ICT Framework programme and EUREKA	Strong expertise in legal and socio-political implications of information an network security/dependability
Cyprus		
Czech Republic		Secure user configuration of industrial systems, security of magnetic measurements, sensors and biometrics
Denmark	Danish Technological Institute (DTI):	Technical consultancy on payment security, designing security solutions tailored to the individual company Dependable system analysis Anti virus Warning and information sharing cryptography
Finland		
France	CELAR (Electronic Centre of Armament) RNRT	Security of information systems Technology of electronic components Electronic war and satellites Information systems telecommunications
Germany	Multimedia projects: FairPay (joint R&D project) VERNET AN.ON ASPIK Biotrust (interdisciplinary pilot project) Dasit February 2002: new IT R&D programme was launched, “Förderprogramm IT Forschung 2006”	Vulnerability analysis Simulation Cryptography System analysis Socio-economic and legal implications of dependability

Country	Main programmes	Main R&D issues
Greece		Information and network security tailored to complex environments Socio political dimensions of information security and CIP Electronic commerce
Hungary		Video teleconferencing, telecottages telework
Ireland		Verification tools and techniques Security in computer supported collaborative systems Cryptography Crisis management Security systems architecture Data secure transmission Virus research Intrusion detection
Italy	CNUCE and ENEA are active in various dependability related international fora (IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance; ENCRESS consortium)	Information and network security Cryptography Security system integration Network vulnerability assessment Legal concerns
Liechtenstein		
Luxembourg		
Netherlands		Multi media Electronic commerce Mobile communication Network technology Tele-education Computer supportive co-operation Knowledge management Crisis and risk management
Norway		Vulnerabilities of society, CIP Security process Secure system integration

Country	Main programmes	Main R&D issues
Poland	PIONEER programme	Fault tolerant and dependable systems Failure detection across distributed operating systems Safety analysis of computerised systems and modelling Analysis of computerised systems Assessment of reliability and survivability of communication networks Priorities for R&D: <ul style="list-style-type: none"> • Computer networks and distributed systems • Parallel processing computer decision support systems • Human computer interaction (HCI)
Portugal		Vulnerability assessment Monitoring and detection Risk mitigation Cryptography Early warning Virus and intrusion detection Analysis of socio-economic and political implications of information security and dependability as a whole
Spain		Intrusion detection PKI Cryptography Digital signatures Watermarking Micropayments Access control Data protection Electronic commerce IP networks security Secure channel coding Error correcting codes for cryptography Secret sharing protocols Primality Pseudo primality Chip card applications e-voting
Sweden		

Country	Main programmes	Main R&D issues
Switzerland		Cryptography Data secure transmission Vulnerability analysis Anti virus software Secure system architecture Critical security analysis Security strengthening methods
United Kingdom	DIRC	System dependability Anti virus Network monitoring Intrusion detection Artificial intelligence Adaptive systems

Tab. 3: R&D Management process outside Europe

Country	Leading R&D actors	Main funding source ⁴⁵	Approaches
Australia	Defence research organisations Technology science parks (at universities)		Strong industry involvement is lacking
Canada	Governmental research centres Partnerships of industry and universities (e.g. CANARIE)	b, smaller funds by g	Co-operative (industry-academia)
Japan			1 partnership between public, private, academia: Next-Generation Internet Zone Promotion Association
People's Republic of China			
United States of America	White House Office for Science and Technology Policy (OSTP) as main co-ordinator	G	Co-ordination approach

⁴⁵ g = government; b = business

Tab. 4: R&D programmes in non-European countries

Country	Main programmes	Main R&D topics
Australia		Cryptography Intrusion detection systems e-commerce (data security)
Canada	CANARIE NRC CRC PRECARIN TPC NCE OCIPEP	Ultra- speed information exchange Wireless and optical and network management Biotechnologies Advanced manufacturing Leading information and communications technologies
Japan	Pilot project of an Internet cash payment system (ICASH) Exotic plan for provision of Internet services via unmanned airships (Christened Sky-Net) Other large-scale projects include: Japan Gigabit Network	main R&D areas: key technologies for network security highly reliable back up systems technology to detect network failure technology to trace unauthorised computer access other issues: digital watermark technology authentication of web-sites secure and reliable transmission of data
People's Republic of China	Torch Programme (leadership: State Science and Technology Commission); aim: commercialise the discoveries made by government research institutes and universities	
United States	Government level: <ul style="list-style-type: none"> • Office of Science and Technology Policy (OSTP) • National Telecommunications and Information Administration (NTIA) • Centre for High Assurance Computing Systems • Defence Evaluation Research Programme Administrations (DARPA) And several academic actors (University of Virginia, Carnegie Mellon University, Purdue, etc)	Intrusion detection Artificial intelligence (and other methods to identify malicious code) Anti intruder methodologies Network reliability System survivability Robustness of CI components and CI themselves Modelling infrastructure responses to attacks/failures Interdependencies identification Localisation of key vulnerable notes

Appendix 3: EU IST Dependability Projects

This appendix contains a brief description of the main European dependability-related R&D projects funded by IST FP5.⁴⁶ The list excludes roadmap projects funded in the eighth and final call of the programme in 2002. Total Commission funding for these projects in FP5 was EUR 29,883,000.

Tab. 5: EU IST dependability projects

Title	Description
Malicious and Accidental Fault Tolerance for Internet Applications (MAFTIA) IST-1999-CPA2 11583	Examines new tolerance paradigms to malicious intrusions and accidental faults in large distributed and heterogeneous systems. Web address: http://www.newcastle.research.ec.org/maftia/
Dependable Scale System Vulnerabilities and Survivability (DSOS) IST 1999 CP2 11585	To develop significantly improved means for composing a dependable system of systems from a set of largely autonomous component computer systems. Web address: http://www.newcastle.research.ec.org/dsos/
Harmonisation for the Security of Web-technologies and Applications (HARP) IST 1999 CPA2 10923	Aimed at developing technologies and tools for the integration of Web oriented security systems. Web address: http://www.ee.ucl.ac.uk/~pants/projects/harp/
Fault Injection for Time Triggered Architecture (FIT) IST 1999 CPA2 10748	To experimentally validate the system concepts of time triggered architecture (TTA), building upon an already developed prototype. Experiments were to determine error-detection coverage of the TTA in a realistic architecture by using different hardware and software based on fault-injection methods. Web address: http://www.fit.zcu.cz/
Automatic Tool for Insertion and Simulation of Fault Tolerant Architectures (AMATISTA) IST 1999 CPA2 11762	Primary objective was to provide a modern solution to the design of fault tolerant circuits and systems. Web address: http://www.cad.polito.it/cooperations/amatista.html
Advanced Design Tools for Aircraft Systems and Airborne Software (SAFEAIR) IST 1999 CPA2 10913	Project aimed at developing a model-based methodology for designing dependable embedded systems. Web address: http://www.safeair.org/
Methodologies and Technologies for Industrial Strength Systems Engineering (MATISSE) IST 1999 CPA2 11435	Explored industrial strength methodologies and associated technologies for the engineering of software-based critical systems to support industry in providing essential services. Web address: http://www.matisse.qinetiq.com/
Building Trust in Networking in Newly Associated States through	The project is intended to foster the usage of European-based security technology in Newly Associated States for the purpose of

⁴⁶ This analysis is based on the following documents: Andrea Servida and Tom Jackson, [European Dependability Initiative: Inventory of EC Funded Projects in the Area of Dependability](#) and Andrea Servida, "Towards Dependable and Survivable Systems and Infrastructures" Presentation available at <http://www.cordis.lu/ist/cpt/cpa4.htm>

Title	Description
the Use of Secure Information Society Technologies (NASTEC) IST-2000-29556	building trust and confidence in the growing application of open networks, as for instance e-commerce, e-administration, e-business and tele-working.
Capacity Utilisation in Cellular Networks of Present and Future Generation (CAUTION)	Aims to design and develop a novel, flexible, highly efficient and scalable system able to control cellular network resources. Web address: http://www.telecom.ntua.gr/caution/start.html
Dependability for Embedded Automation Systems in Dynamic Environments with Intra-site and Inter-site Distribution Aspects (DEPAUDE) IST 2000 25434	Aims to develop a methodology and an architecture to improve dependability for non-safety critical, distributed, embedded automation systems with both IP (inter-site) and dedicated (intra-site connections) Web address: http://lesbos.esat.kuleuven.ac.be/depaude/
Dependability Benchmarking (DBENCH) IST 2000 25425	Defines a conceptual framework and an experimental environment for benchmarking dependability of commercial-off-the-shelf systems. Web address: http://www.laas.fr/Dbench/
Experimentation of a Monitoring and Control System for Managing Vulnerabilities of the European Infrastructure for Electrical Power Exchange (EXAMINE) IST 2000 26119	Aims to develop information technology to improve the security of the electronic power system, and to establish the basis for a real time control strategy to be adopted Europe-wide. Web address: http://www.ree.es/examine/home_page.htm
A Platform for Risk Analysis of Security Critical Systems (CORAS) IST 2000 25301	CORAS aimed to develop a framework for precise, unambiguous, and efficient risk analysis of security critical systems. Web address: http://www.nr.no/coras/
Computing Systems Architecture Network (CABERNET) IST 2000 25088	A network of excellence among the leading European and international experts in the areas of dependability. Web address: http://www.newcastle.research.ec.org/cabernet/
Wireless Trust for Mobile Business (WITNESS) IST-2001-32275	Witness contributes application-level security for Mobile Business to 3 rd Generation Wireless Networks.
Computer-Aided solutions to Secure Electronic Commerce Transactions (CASENET) IST-2001-32446	CASENET will develop methodologies and tools to build secure and reliable protocols for transactions involved in e-commerce and e-government applications.
(SAFEGUARD) IST-2001-32685	SAFEGUARD aims to enhance the dependability and survivability of Large Complex Critical Infrastructures (LCCIs), such as distributed electric and telecommunication networks.

Title	Description
	The main objective is to provide a systemic conceptual framework and an integrated software toolkit that, employed within an intelligent multi-agent system, enhance the dependability and survivability of Large Complex Critical Infrastructures (LCCIs), including the underlying Networked Information Intensive Systems (NIIS).

Appendix 4: EU IST Dependability Roadmaps

The following roadmap projects received funding from the final call of the FP5 IST programme. They started their activities in or about July 2002 and are expected to last around 12 months. Preliminary results will be presented at the IST 2002 conference in Copenhagen, at the beginning of November.

Financial constraints prevented the Commission from funding roadmaps in other priority dependability related areas, notably:

- Protection of electronic content and digital rights management
- Network security, including warning and information sharing
- Security issues related to the sharing of distributed resources such as peer-to-peer networking or the global GRID computing infrastructure.⁴⁷

Tab. 6: EU IST Dependability Roadmaps

Title	Description
Analysis and Assessment for Critical Infrastructure Protection (ACIP)	Focuses upon methods for developing models and simulations for analysis of Large, Complex, Critical Infrastructures
Roadmap for Advanced Research in Privacy and Identity (RAPID)	Focus upon privacy and identity management. Particular attention upon new technological and communication environments such as mobile commerce.
Accompanying Measure System Dependability (AMSD)	Examines a full-range of dependability related activities. This will provide a basis to develop an R&D roadmap to be implemented during FP6.
Pioneering Advanced Mobile Privacy and Security (PAMPAS)	Explores the technological challenges to providing security, privacy and identity management functionalities over mobile devices. Particular attention to issues such as cryptography, privacy enhancing technologies, PKI, digital rights management.
Roadmap to Successful Deployments from the User and System Integrator Perspective (BIOVISION)	Contributes to the development of a comprehensive R&D roadmap for the secure, user-friendly, socially acceptable and ethical use of biometrics.
Roadmap for European research on Smart Technologies (RESET)	A roadmap for future R&D strategies in smart-card related technologies and applications.
Strategic Roadmap for Crypto (STORK)	Aims to consolidate the European research community involved in crypto-related activities in devising a detailed strategic roadmap.

⁴⁷ Information from Max Lemke, "Roadmap Projects Related to Trust and Security", Presentation at Workshop for the Preparation of the First Calls of FP6-Trust and Security, Brussels, 30 May 2002, available at <ftp://ftp.cordis.lu/pub/ist/docs/irg-tc-present.zip>

Appendix 5: Dependability R&D Topics

A number of projects have sought to identify and prioritise R&D to support information infrastructure dependability. The DEPPY website provides a comprehensive guide to European Union activities. The most significant work is reflected in the following list:⁴⁸

- [1] *Policy Paper*; IAAC Research and Development Working Group; April 2001
- [2] *Research and Development for CIP*; IAAC seminar, 15 November 2001; IAAC
- [3] EU-US Workshop Report; R&D Strategy for a Dependable Information Society: EU-US Collaboration, DDSI⁴⁹
- [4] Mastering the Vulnerabilities of Information and Interdependent Infrastructures: Towards an RTD roadmap for Framework Programme 6; Report from Meeting of the EU Working Group on Information Infrastructure Interdependencies and Vulnerabilities; Version 3; 17th November 2001
- [5] DDSI Work Package 1.2 – Part A: “Global Overview: Countries, International Organisations and Inter-Governmental Organisations”, Version 1.0, June 2002
- [6] Report on the Federal Agenda in Critical Infrastructure Protection Research and Development – Research Vision, Objectives, and Programs; Critical Infrastructure Protection R&D Interagency Working Group; January 2001
- [7] *Trust and Security*; Contributions from the FP 6 Internal Reflection Group, Draft Version 3.0; June 2002
- [8] Andrea Servida and Marcelo Masera, “Workshop on Dependability in Information Society: Future Scenarios and R&D Challenges, LAAS-CNRS, Toulouse, 12-14 December 2001
- [9] *Thèmes de recherche sur la sécurité des systèmes de télécommunications*, RNRT, France

This appendix groups the recommendations of these roadmap efforts under seven headings, some with subheadings as indicated:

- Policy Issues
- Basic Research
 - Interdependencies
 - Threats and risks
 - Security implications of technological developments
 - Other Aspects
- The Human Factor
 - Users/Customers
 - Service Providers and Vendors
 - Other

⁴⁸ The numbers in brackets will be used to identify the documents as sources in the tables prepared in this appendix.

⁴⁹ available at <http://www.ercim.org/EU-NSF/DIS.pdf> or via http://www.ddsi.org/DDSI/other_events.htm

- Economic Aspects
- Technical/Technological Measures and Capability Issues
 - Protection
 - Detection
 - Reaction
 - Other
- Organisational Measures
- Measurement, Simulation and Testing

The following tables also reflect the prioritisation and timescales where these were available from the sources.

Tab. 7: Policy Issues

Research Topic	Priority	Time frame	Source
Standardisation:	Priority	Med.	[1]
• Interoperability and standardisation	-	-	[4]
• Ease deployment and integration of new business models along value chains and crossing current infrastructure limits	-	-	[4]
• Framework to influence design and development of systems embedding identity requirements (balanced with personal data protection)	-	-	[4]
• Transatlantic harmonisation of dependability / security concepts and language	Priority	Med.	[1]
• Inter-model data exchange	-	-	[6]
Global frameworks and ISACs	Priority	Med.	[1]
Collaborative R&D	Priority	Med.	[1]
• To develop privacy enhancing technologies to knowingly and efficiently manage personal and virtual identity in digital transactions	-	-	[4]
Funding models to enable research (e.g. Public private funding models)	Priority	Med.	[1]
Legislative requirements (national, regional, sectoral, global)	Priority	Med.	[1]
The roles of government and private sector	Priority	Med.	[1]
• Growing role of industry in controlling CNI, reduction of government's power to influence the provision of CNI	-	-	[1]
• Public private co-operative models	-	-	[1]
• Examinations of the barriers between government and industry stakeholders in sharing CIP-related information	-	-	[6]
Cyber-crime counter measures	Priority	Med.	[1]
Law enforcement	Priority	Med.	[1]
Security engineering as a new education and career option			[3]
Developing comparable knowledge throughout the EU (partnerships among academia and practitioners)			[4]
Promoting more application/threat-driven R&D (less technology-driven)			[3]
Education	Priority	Med.	[1]
Awareness raising for dependability issues – creating an environment in which there is demand for corresponding products and services			-

Tab. 8: Basic Research: Interdependencies

Research Topic	Priority	Time frame	Source
Interdependency Analysis	-		[6]
• Infrastructure connections within a sector	-		[6]
• Infrastructure connections between different sectors	High		[6]
• Growing interdependencies between essential infrastructures	-		[3]
• Micro & macro dimensions	-		[4]
• Key interdependencies between energy and information	-	Short	[4]
Continuity and viability of the information infrastructure		Med. to long	[6]
Barriers in protecting LCCI			[6]
Consequence analysis and management			[6]
Reliance on unique, hard to procure equipment and materials			[6]
Theoretical framework for understanding and predicting the nature of interdependencies and their effects on a country as a whole			[6]
Locating key vulnerable nodes / components / systems			[2]
• Develop methods to model interdependencies of LCCI to identify the critical sub-networks			[3]
• Simulate behaviour of critical subnetworks under different attack scenarios			[3]
Characterisation of foreign influences on infrastructures			[6]
Systems modelling, in particular complex systems, interdependencies and criticality	Priority	Short to med	[1, 3, 4]
Diversity of organisations and resources used to provide CNI			[1]
Modelling and simulation of interdependencies and vulnerabilities			[4]
Managing critical dependencies upon global services / relying on open networks for control applications			[1, 3]
Role of autonomous embedded systems and sensor networks for dependable architectures			[3]
Susceptibility to cascading failures among LCCI			[6]
Survivable subnetworks embedded within a LCCI			[3]

Tab. 9: Basic Research: Threats and Risks

Research Topic	Priority	Time frame	Source
Threat, vulnerability and risk identification and assessment	High		[1, 6]
Threat identification and assessment (e.g. predictive techniques for threat assessment)		Short	[4, 1]
Malware evolution prediction	Priority	Med.	[1]
Identification of vulnerabilities in real-time control technologies			[3, 6]
Physical vulnerabilities	Priority	Med.	[1, 6]
Systems response to catastrophic failure	Priority	Med.	[1]
Reliance on rapid access to accurate information			[6]
Electronic attacks on information networks			[2]
Tracking developments in Information Warfare	Priority	Med.	[1]
Response to short term threat	Priority	Med.	[1]
Susceptibility to disruption of LCCI elements			[6]
Malicious attacks		Short	[4]
Security of automated infrastructure control systems	Priority		[6]

Tab. 10: Basic Research: Security implications of technological developments

Research Topic	Priority	Time frame	Source
Mobile code and agents			[1, 6]
Real-time control technologies			[6]
Universal, always-on broadband access			[2]
Wearable computing			[2]
Personal Area Networks			[2]
Quantum computing	Priority	Med.	[1, 2]
Wireless systems			[2]
Ubiquitous computing			[1, 2]
Data fusion			[2]
Universal personal identification and authentication techniques			[1, 2]
On-line services, e.g. government			[1]
Homogeneity of software and hardware			[1]
Outsourcing			[1]
Dependability challenges from network's increasing bandwidth and latency	Priority		[4]
Adequate understanding of risks and vulnerabilities for privacy in e-transactions	Priority		[4]
Security in mobile networks: <ul style="list-style-type: none"> • Mobile routers • Secure multicasts communication • Efficient and transparent charging mechanisms in the presence of multiple payment schemes • Security policies and authorisation associated with different administrative domains • Specification of requirements for security and privacy • Development and integration of "trusted components" • Defining and managing privacy policies to permit access to location-sensitive services respecting user's privacy • New evaluation profiles • Rich authorisation / delegation infrastructure supporting several levels of certificates and different roles and privileges 			[4]
Peer to peer environment			[4]
Reliability & security in future computational grids		Short to med	[3]

Tab. 11: Basic Research: Other Aspects

Research Topic	Priority	Time frame	Source
“Best Practices” to use for limiting vulnerabilities			[6]
Long range scenario planning		Med.	[1]
Identity management			[4]
Criteria for choosing open or private networks		Short	[4]
Classification of attackers' behavioural types and development of motivation methods and activities to avoid destructive actions (including education, laws, etc.)			-

Tab. 12: The Human Factor: Users/Customers

Research Topic	Priority	Time frame	Source
Human factor analysis on security systems			[6]
(Sufficient) adoption of technology	Priority	Med.	[1]
Adequate educational initiatives, e.g. Providing end user with elements for understanding the risks, expressing their preferences and risk management	Priority	Med.	[1, 4]
Privacy, e.g. user control on personal data and personal trusted components	Priority	Med.	[1, 4]
(Avoidance of) social exclusion	Priority	Med.	[1]

Tab. 13: The Human Factor: Service Providers and Vendors

Research Topic	Priority	Time frame	Source
Designing security into software and systems	Priority		[1, 2, 4]
Industry self-regulation for combating computer crime	Priority		[1]
Orientation towards privacy in systems and infrastructure	Priority		[4]
Technology measures supporting law enforcement and accountability	Priority		[4]
Developing and applying dependable system architectures		Long	[4]
Understanding user's QoS demands		Long	[4]

Tab. 14: The Human Factor: Others

Research Topic	Priority	Time frame	Source
Education and training of research personnel in CIP R&D	High		[6, 3]
Ethics in IT	Priority		[1]
Understanding of distributed information assets			[4]
Human Centric Systems	Priority	Med.	[1]
Risk perception and education at all levels			[4]
Public perception, individual perception			[4]
Trust and confidence building <ul style="list-style-type: none"> • Confidence in services and capabilities to deal with problems (incl. worst cases) • Building trust on the operators of the infrastructures and the systems 		-	[1]
Identifying and understanding (emerging) end-user requirements			-
Classification of user behavioural types (w.r.t. responsible acting) and development of motivation methods (including education, laws, etc.)			-

Tab. 15: Economic Aspects

Research Topic	Priority	Time frame	Source
Promoting security in COTS products, e.g. stimulation for developing security / dependability in products			[1, 2]
Characterisation of information assets and their relative quality according to each business context			[4]
Support to make-or-buy decisions		Short	[4]
Single integrated methodology linking business and technology			[1]
Impact of economics on information assurance & dependability		Short to med	[3]
Bridging gap from risk and dependability system tools / methods to high-level business process requirements			[4]
Valuing information assets: <ul style="list-style-type: none"> • Consistent methodologies and reference standards in particular for distributed assets in networks outside the direct control of who can be affected by them • Methods for business environment 			[4]
Developing realistic service level agreements (SLAs) and standards so contracts can be made clearer / comparable			-

Tab. 16: Technical/Technological Measures and Capability Issues: Protection

Research Topic	Priority	Time frame	Source
Security of automated infrastructure control systems	High		[6]
Protection of Critical Infrastructures:			
<ul style="list-style-type: none"> Reducing vulnerability to terrorist acts Identification of infrastructure vulnerabilities and their translation into security requirements 			[6] [4]
Robust I&C control systems			[6]
Secure supervisory control and data acquisition systems			[6]
<ul style="list-style-type: none"> Authentication & Authorisation Privacy awareness Personal and business transactions in multi-party and privacy-hostile environments 	Priority	Med.	[1] [4] [4]
Multi-layer approach to security and survivability:			
<ul style="list-style-type: none"> From network to application layer Responding to multiple stakeholder needs (service providers, content providers) that are user friendly, flexible and adaptable 	Priority		[4] [4]
Cryptography:			
<ul style="list-style-type: none"> Cost effectiveness PKI Encryption New applications (e.g. to combat DoS-attacks) 			[2] [6] [6] [2]
Security architectures			[2, 4]
Physical protection			[6]
Technologies & mechanisms to enforce dynamic security policies for heterogeneous and changing architectures			[4]
Chaining trusted resources			[4]
Interoperability of security mechanisms among heterogeneous networks and their impact on performance requirements	Priority		[4]
New Access control techniques			[4]
<ul style="list-style-type: none"> Role based Rule based Privacy aware 			
Secured transfer of data through legacy systems			[4]
Watermarking robustness			[4]

Tab. 17: Technical/Technological Measures and Capability Issues: Detection

Research Topic	Priority	Time frame	Source
Intrusion Detection	High		[1, 6]
Steganographic detection	Priority	Med.	[1]
Monitoring	High		[6]
Network alarm systems			[6]
Multi-sensor technologies			[6]
Failure warning technologies			[6]
Technology to support large scale networks of intrusion detection monitoring			[2]
Distributed attack detection			[4]
Better methods of accountability tracing			[6]
Installation of increased and effective early-warning mechanisms			[6]

Tab. 18: Technical/Technological Measures and Capability Issues: Reaction

Research Topic	Priority	Time frame	Source
Intrusion Response, e.g. methodologies for containing, stopping or ejecting intruders			[2, 6]
Disaster recovery:			[2, 4, 6]
• Data recovery			[2, 4, 6]
• Service recovery	Priority	Med.	[1]
• Reconstitution of damaged or compromised systems	High		[6]

Tab. 19: Technical/Technological Measures and Capability Issues: Other

Research Topic	Priority	Time frame	Source
Information assurance	High		[2, 6]
Scalable, network based I.A. capabilities decoupled from underlying infrastructure	High		[1]
Forensics	Priority	Med.	[1, 4, 6]
Addressing identified vulnerabilities and shortcomings			[6]
Biometrics			[2]
Scalable technologies, e.g. for trust services	Priority	Med.	[1, 2]
Alternatives to monitoring traffic in transit	Priority	Med.	[1]
Technology migration, interoperability, legacy	Priority	Med.	[1]
Human computer interaction (HCI)	Priority	Med.	[1]
Transparent fault tolerance			[3]
Network awareness technologies			[4]
Growing demand for “working and affordable dependability” for open information infrastructures and unbounded IP networks	Priority		[4]
Support for paradigm shift from “resist to attack” to “survive and adapt”	Priority		[4]
Multidimensional models (covering behaviour, composition, physical elements, etc.) for designing a language to describe dependability of unbounded systems and infrastructures	Priority		[4]
Multiparty transactions			[4]
Robustness / Survivability:			
• Robust open source software	-		[4]
• Service continuity	Priority	Med.	[1, 2]
• Intrusion tolerant systems	-		[1]
• Intrusion tolerance for large, dynamic ad hoc/peer-to-peer groups	-		[3]
• Contain, mitigate and defend against effects of disruptions	-		[6]
• Attack tolerant networks	Priority	Med.	[2]
• System survivability	-		[1, 6]
• Emergency modes in communication systems	-		-

Tab. 20: Organisational Measures

Research Topic	Priority	Time frame	Source
Coordinated process for collecting and distributing vulnerabilities and threat information to developers, operators and users			[6]
Response and recovery procedures			[6]
Centralised approach for assuring safety and security of CI structures			[6]
Managing control of information on vulnerability assessments			[6]
Establishment of a non-governmental Institute for Information Infrastructure Protection	High		[6]
Risk management <ul style="list-style-type: none"> • Consequences of dissonance of perceived threats and actual causes of failures / computer damage • Incorporation of human factor • In open environments • Developing a mapping of the available governance mechanisms for dependency analysis and risk management 			[1, 4, 6] [3] [2] [4] [4]
Independent EU biometrics assessment / certification centre	Priority		[4]
Trans-national network of independent Emergency Management centres			[4]
Disaster management			[1]
Maintenance of critical systems by non-trusted organisations		Short to med	[3]

Tab. 21: Measurement, Simulation and Testing

Research Topic	Priority	Time frame	Source
Metrics for: <ul style="list-style-type: none"> • benchmarking security solutions • measuring the scale of impacts of interdependency-related disruptions • prioritisation of remediation 	Priority		[1, 2, 4] [6] [3]
Tools for realtime patterns and analysis of open network traffic data			[4]
Interaction and trade-offs between different assurance techniques	Priority		[4]
Auditing & testing of robustness	Priority	Med.	[1]
Modelling and simulation: <ul style="list-style-type: none"> • Real-time programs • Techniques and tools • Real-time dependability and continuity analysis • Large scale and composable modelling and simulation capabilities • Traffic modelling for security activities • Infrastructure responses to attacks or failures • Requirement for modelling of attackers 		Short	[6] [3, 4] [4] [4] [4]
Capabilities to adequately and realistically test new methodologies and technologies			[6]
Certification / Verification: <ul style="list-style-type: none"> • Revised certification procedures in aviation sector (current design of dependable systems / processes ahead of certification/verification processes which assume hard-coding) • Dependability certification on international level • For product and security systems of a level of protection by an independent authority • High-dependability applications 		Short to med	[3] [3] [4] [1]
Validation procedures and techniques		Short to med	[3, 6]
Common Terminology		Short to med	[3]
Methods for identifying malicious code in operating system code			[2]
Vulnerability / risk assessment: <ul style="list-style-type: none"> • Formal tools • of software architectures • Integrated business and technology methods 			[2]

Dependability Development

DDSI

Support Initiative

DDSI

DDSI
IST-2000-29202

For more information on the project DDSI,
please visit

www.ddsi.org

Project number IST-2000-29202,
supported by
the IST research programme
of the European Community,
managed by
the European Commission DG
Information Society.

