Dependability

European Commission -
US National Science Foundation

Strategic Research Workshop

R&D Strategy for a

Dependable Information Society

Düsseldorf, Germany,
1-2 December 2001

Workshop Report and
Recommendations

EC-NSF WORKSHOP REPORT

R&D STRATEGY FOR A DEPENDABLE INFORMATION SOCIETY: EU-US COLLABORATION

1 – 2 December 2001, Düsseldorf, Germany

Report Version:	1.0
Report Preparation Date	8 April 2002
Dissemination Level:	Public

Title:	EU-US Workshop on R&D Strategy for a dependable Information Society: EU-US Collaboration. *Report of a Workshop held in Düsseldorf, 01-02 December 2002*
Abstract:	The report provides a summary of the workshop discussions and conclusions
Status	Final
Date:	08 April 2002
Authors:	Susanne Jantsch and Christine Schwarz-Hemmert, DDSI, IABG Andrew Rathmell, DDSI, King's College London
Distribution:	Public

This report was prepared by the Dependability Development Support Initiative (IST-2000-29202)

We invite readers of this report to send comments to:

Susanne Jantsch DDSI jantsch@iabg.de	Andrew Rathmell DDSI andrew.rathmell@kcl.ac.uk
Andrea Servida EU andrea.servida@cec.eu.int	Marc LeBlanc US Department. of State LeBlancME@T.state.gov

Executive Summary
EU-US collaboration on dependability for the Information Society
EU-US Workshop 1 – 2 December 2001

This workshop on the EU-US collaboration on dependability for the Information Society was jointly organised by the IST Programme of the European Commission and the US Department of State with the logistics provided by the DDSI project (Dependability Development Support Initiative), which is partially funded by the IST Programme. The workshop was held on 1-2 December 2001 in Düsseldorf, Germany.

Building on previous workshops and meetings, the aims of the workshop were to discuss i) collaboration between the EU and USA on R&D for information infrastructure dependability and to ii) roadmap priority areas for future collaboration. The workshop brought together around 20 participants from the EU side matching around the same number from the US side. The participants from government organisations responsible for research and policy in the area (about 25%) were complemented by academic and industrial representatives participating in the respective research programmes. The meeting was co-chaired by the US State Department and the EC.

The current situation related to the topic of dependability and EU-US RTD collaboration was identified as follows:

- There is a variety of programmes related to the broad topic of dependability available in the US. The individual objectives of these programmes are linked to the respective objectives of the agencies through which they are supported (DoE, DARPA, NSF, …). Related to international co-operation of the agencies, the State Department is orchestrating the initiatives. On the EU side, the US programmes are matched by the dependability initiative under the IST Programme of the European Commission and several initiatives in Member States. The latter were not subject of the meeting. On both sides regulatory and legal frameworks are in strong relation to the Research Programmes.
- In the area of dependability in a broad sense, several collaborations between actors on both sides of the Atlantic are on-going, e.g. direct collaborations between organisations and projects on both sides of the Atlantic, workshops between projects to exchange experiences, or broader workshops to define potential research agendas for specific aspects related to dependability. A framework for collaboration is given by the EU-US Science & Technology Agreement.
- In the last years several workshops and conference sessions were held within this framework addressing various aspects of dependability and EU-US collaboration. These events have contributed to a relationship of trust between the involved government, academic and industrial organisations. Through the tragic events of 11 September 2001, the topic of dependability and in particular aspects related to vulnerabilities of critical infrastructures and interdependencies have received increased attention by policy makers, politicians, and internal and external security bodies. As a result, a need for concerted efforts and complementary international collaboration on complex global problems requiring global solutions has been highlighted on both sides.

In order to further the EU-US collaboration the following challenging objectives for the parallel working groups of the workshop were set:

(1) Identify potential areas for EU-US collaboration in the context of dependability based on the developed strength of the respective research and industrial communities;

(2) Develop first ideas of what should be done as to be ready for concrete actions at the beginning of the EU 6th Framework Programme;

(3) Identify and analyse detailed research topics in the context of dependability going beyond a "shopping list":

  - Identify research needs and gaps on both sides and possibly establish a mapping;
  - Find a balanced approach between being pushed by technologies and being pulled by application-scenarios;
  - Identify the constituencies at all necessary levels of the value chain;
  - Identify the concrete added value/need for EU-US collaboration going beyond generic statements.

As a result, the participants developed a comprehensive list of potential topics for collaboration related to dependability aspects. In order to get a larger scale EU-US collaboration off the ground, it was agreed that as a preparatory step a stronger effort was needed to answer the above questions and thereby focus and concretise a future collaboration making it beneficial for both sides.

In this context it was suggested that a "steering group" be put in place, which would address the above concrete questions. This group would have to be constituted by representatives from academia and industry in the EU and the US supported by the respective funding bodies. In order to allow for sufficient effort to be invested, participants to this steering group would have to be financially supported through the relevant funding mechanisms on both sides. On the EU side, for example, a Thematic Network Proposal submitted under the Action Line on Strategic Roadmaps of Key Action II of the 5th Framework Programme was identified as an appropriate mechanism.

In addition to this "steering group", the academic and industrial participants recommended to the officials from both sides to assure that future collaboration is facilitated by

- jointly laying down the ground rules;
- enabling joint proposals;
- avoiding double procedures;
- simplifying funding mechanisms.

As a conclusion the participants agreed that these steps forward should be taken quickly in order to keep the pace resulting from the attention to the topic after the tragic events of 11 September and this workshop.

Workshop presentations will be available at deppy.jrc.it (also via www.ddsi.org)**.**

Table of Contents

1 Background

The EU-USA Science & Technology agreement was signed in Washington on the 5th December 1997. Within that agreement both parties have expressed their appreciation of the global scope of the Information Society, its infrastructure and its dependability concerns. There is mutual concern in these areas and they provided a rationale for exploring joint research projects.

In June 1998, a Conference on 'New Vistas in Transatlantic Science & Technology Cooperation took place at the National Academy of Sciences in Washington. Subsequently a task force was established under the US/EU S&T Agreement to examine Information Society and CIP R&D issues. The task force has sponsored a number of workshops and conferences. At the workshop in Venice (20 – 21 April 1999), the objective was to identify themes that would benefit from R&D collaboration.

The Venice workshop concluded by identifying the rationale for global collaboration as being a response to the globalisation of information infrastructures and services. In this globalised system, similar dependability concerns necessitate joint approaches in order to enable better use of a limited pool of skills and experiences. The workshop identified general areas for collaboration and facilitated information exchange about general concepts, methods, approaches and research models.

The initial collaboration mechanisms would focus on the fostering of the exchange of information and the identification of bilateral procedures compatible with current EU-USA research schemes. Further dialogues during IST 1999 occurred at Helsinki (21 Nov 1999) on the practical procedures for research collaboration between Europe and the USA, which at that stage was focussing on CIP whilst Europe addressed the 'dependability' areas. At Helsinki, the "Venice" recommendations were progressed by sharing information on concrete work and research programmes in the EU and the USA. It was agreed to maintain the inventories of dependability related projects in the EU and the USA thus started and to provide information sharing facilities for use by officials and researchers involved in the collaboration.

A further workshop on 'Information Assurance and Survivability' was held at DERA Malvern in June 2000. As part of the predominantly technical exchange, the IST MAFTIA project presented five papers on the work packages and methods being used. In return the US covered IA S&T progress in the US.

The Düsseldorf workshop was convened with the intention of further deepening the Transatlantic effort to define research policies and promote collaborative working on dependability and critical infrastructure protection R&D.

The agenda and list of contributions to this workshop (see Annex 1 and 2) reflect the successful take up of the ideas from the former workshops. Workshop participants in Düsseldorf examined not only specific research topics and projects but also discussed the need for implementing mechanisms for closer collaboration.

For the EU side, the workshop was also an opportunity to examine how the forthcoming 6th Framework Programme (FP6) could facilitate improved international collaboration, the events of 11 September 2001 having added further US urgency to the relevance of these activities.

2 Aims and Objectives

The workshop brought together individuals responsible for and participating in relevant research programs. The aims of the workshop were to discuss requirements for wider collaboration and to identify conditions that future research programmes should provide to enable future joint work in the interrelated fields of dependability, information assurance, and critical infrastructure protection.

One part of the workshop was dedicated to sharing detailed information on present and future R&D efforts in these fields as well as on the structures of existing and planned research programmes. Another part of the workshop was designed to allow researchers to present their views of where and how US-EU collaboration could provide benefits and synergies.

The primary motivations for the workshop were:

- Promote more application/threat-driven R&D (less technology-driven);
- Allow identification of all constituencies in the value chain (US and EU) who need to be involved;
- Allow identification of real added value of US-EU collaboration;
- Seek opportunities and identify models for joint research in FP6 and current / upcoming US research programs.

The workshop results are presented in two sections to this report:

- an agenda for collaboration summarising main conclusions and recommendations as well as specific collaboration topics addressed during the workshop,
- the proceedings giving an overview of the contributions to and the discussions of the workshop.

3 Agenda for Collaboration

3.1 Rationale for collaboration

The rationales for international collaboration developed in the Venice Workshop of April 1999 were reaffirmed in Düsseldorf.

To enable such collaboration, the differences between the research communities need to be analysed and understood to identify factors that will support collaboration. These differences are based partly on the different organisational structures of the USA and the EU and partly on the differing degrees of maturity of the policy frameworks in the USA and the EU.

Among the drivers for international approaches to R&D in dependability and information assurance are the understanding that:

- these are international issues that can no longer be addressed on a national basis;
- embedded systems are becoming increasingly networked and more complex;
- interdependencies are growing between essential infrastructures.

3.2 Motivations and Requirements

Participants addressed the following motives for collaboration:

- a shared vision of the future requiring dependability, leading to a requirement to gain mutual understanding
- 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
- community building, e.g. focused international communities of interest on specific problems
- improved access to relevant data that is not available nationally.

The discussions also expressed a need for commonly understood requirements and specifications, including a need for language harmonisation and development of common terminology. A complementary effort might be to provide taxonomies from different communities (e.g. dependability and information assurance) in a form easier to understand for an “outsider”.

3.3 Collaboration Areas

A few examples of already successful collaboration were identified:

- MAFTIA/OASIS
- Clustering stimulation initiative

- Embedded & Hybrid Systems Research

These successes were achieved despite the lack of a suitable framework, and were made possible by common interests amongst researchers. For more systematic collaboration, the following requirements were identified:

- Common R&D Strategy
- Joint Project Model in FP6
- Funding Framework

The following propositions of areas for possible future collaboration (short to mid term) were discussed:

- Modelling of interdependent utilities (e.g. energy, telecommunications,…)
- Impact of economics on information assurance & dependability
- Dependability certification – required on the international level
- Large scale networked embedded systems involving people (pervasive computing)
- Socio-technological issues in global computer-based systems
- Maintenance of critical systems by non-trusted organisations
- Reliability & security in future Computational Grids
- Creation, e.g. by abstraction, and analysis of multi-level models of large systems
- Trustworthy, dynamic, complex information sharing
- Model-based adaptation for e.g.
  - Intrusion detection / fault detection
  - Reconfiguration
- Intrusion tolerance for large, dynamic ad hoc/peer-peer groups and further new approaches to intrusion detection
- Common Terminology
  - support for clear thinking and communication
  - convergence of dependability and security concepts of languages
  - transatlantic harmonisation of dependability / security concepts and language
- CIP design
  - Development of measures to specify unambiguously the properties required in a critical infrastructure design
  - Development of design principles and techniques for achieving dependable CIP designs

- Validation procedures and techniques
  - validation of systems that must survive rare failure events is challenging, requires special techniques (e.g. quantify the absolute effectiveness of particular techniques)
  - identification of appropriate measures of tolerance, e.g. for intrusion
  - requirement for modelling of attackers / attacks

  As a possible approach, a combination of different techniques may include:
  - formal methods
  - probabilistic methods
  - experimental
  - red teaming
- Dependable Information sharing

  The requirement for this field derives from applications as different as virtual enterprises or complex Command & Control systems. Issues to be examined include:
  - Understanding of component relationships/ interdependencies
  - Role-based access control / policy complexity management

One clear gap in currently ongoing research activities was identified and added to areas for collaboration, namely: **Metrology**. The needs here are

- a widely accepted basis for data collection and measurements of accidental and malicious events
- exploiting measurement trends for sustaining current and future research in e.g. identifying existing gaps or expected future threats.

Another field for collaboration suggesting the need for new approaches is **education**. Some examples were given

- Security engineering as a much needed, possible new research career
- Share and re-use successful / outstanding elements of educational programmes to enhance course qualities
- Virtual University

3.4 Collaborative Frameworks

To enable collaboration on these and other topics that will emerge involving groups from both the US and the EU requires regular opportunities (and funding) to meet in order to identify concrete fields for collaboration as early as possible.

From the US side, DARPA and NSF already have possibilities to fund non-American participants. From the EU side it was pointed out that the 6th Framework Programme may offer some flexibility to enable wider participation of non-EU research groups in future EU proposals. In addition to these

approaches, a clear wish to initiate a formal EU-US framework for collaboration was expressed. The following steps were suggested:

- Proposed framework for EU-US work
  - minimalist steering group
  - stimulation of clustering and close co-operation (e.g. by staff exchanges)
  - provision of technical aids

The objectives of such a framework should comprise

- Identification of suitable topics[1]
- Laying down ground rules
- Enabling joint proposals and / or participation of US in EU proposals and vice versa.
- Avoidance of double jeopardy

There are already examples of collaborative EU-US models which may provide a basis to develop the required conditions for collaboration e.g. by applying established procedures to US-EU collaboration or by wider internationalisation of existing bi- or multilateral models.

3.5 Other aspects

Participants also pointed out that there are other communities where needs for increased information exchange and collaboration will arise, such as legal aspects / law enforcement. The G8 activities on cyber-crime yield a good example of how such sharing might take place.

[1] The list of “Collaboration Areas ” above (3.3) provides a basis.

4 Proceedings

4.1 Introductory Position Statements

In the first part of the workshop, position statements were presented and discussed in order to provide an overall understanding of intended developments both in the EU and the US[2].

- 6th Framework Programme in the EU will introduce the opportunity for large integrated projects.
- National Strategy for Critical Infrastructure Assurance in the US has been advanced by new measures to address threats:
  - Executive order establishing Homeland Security Office
  - Homeland Security Presidential Directive 1
  - Executive Order for CIP in the Information Age (replacing PDD 63)

The discussions that followed covered various research programmes in the US and the EU. These may be summarised by the following statements:

- Dependability for the information society will be a key issue
- There is a need to identify research needs, gaps and more application-driven approaches
- There is a need to identify and include all constituencies affected and involved
- There is a need to reinforce research and excellence, outreach and awareness, dialogue and co-operation
- There is a need to make use of new initiatives started or enhanced as a consequence of the September 11 terrorist attacks

Plenty of motivations for more systematic collaboration were identified, among them the fact that globalisation of services and applications leads also to globalisation of problems, which should therefore benefit from the same solutions wherever they occur. This becomes of increasing importance if solutions are needed fast, since duplication of effort wastes time and resources.

There are political, cultural and other barriers which have to be identified and taken into account, but there are already examples of large international collaboration, e.g. for telescopes or space programmes, that prove that such barriers can be overcome.

Drivers for international collaboration are expected to arise from e.g. cyber security and privacy, financial and e-commerce dependability, communications infrastructure survivability, shared national security technology against all forms of terrorism.

Obstacles to be dealt with include different objectives, timetables, priorities, different fiscal years, different intellectual property rights, double and triple jeopardy, need to meet multiple guidelines for joint research.

[2] Annex 2 lists the presentations to this topic under “Dec 1, plenary”

In the EU, project DDSI could provide contributions to both identifying areas that need to be addressed to enable not only complex research programmes, but also successful international implementation by fostering common visions for community builders and the identification of public policy needs, as well as by supporting development of partnerships and of an R&D roadmap.

4.2 Working Groups

In the second part of the workshop, two working groups were convened. Both groups started with presentations (see Annex 2), followed by discussions.

4.2.1 WG 1: Information Assurance

The discussions of the working group were stimulated by four contributions, beginning with a short address on the MAFTIA project and the successful collaborations between MAFTIA on the European side and OASIS on the US side.

The subsequent discussions raised several approaches and issues in the dependability of complex systems, e.g.:

- the roles of probabilistic and formal methods modelling
- information assurance requirements of an integrated supply chain from the supplier to the customer as an example of a complex system on which manufacturing of complex products is based
- intrusion tolerance of large peer to peer systems
- security engineering as a possible new education and career option
- possible role of validation and the resulting need for shared methodology, combining and reconciling methods and approaches
- Dissonance of perceived threats and actual causes of failures / computer damage. Consequences for risk management?

According to the group, important research needs and gaps that could be the subject of collaborative work include the topics of validation, metrology, and terminology. It was also agreed to be important that research programmes that enable collaboration should extend from research to implementation and industrial pull-through.

4.2.2 WG 2: Interdependencies

This WG based its discussions around a number of presentations, which are available on deppy.jrc.it. This section highlights the topics discussed:

Open networks: how can we rely on them for control applications?

- role of autonomous embedded systems and sensor networks for dependable architectures
- scenario exercises
- modelling and remediating interdependency

Research Issues in Dependable Real-time Systems

- composability
- secure real-time systems
- transparent fault tolerance
- certification of high-dependability applications
- domain-specific architectures

Dependability of Networked Embedded Systems

- Need to revise certification procedures in the aviation sector since current design of dependable systems/processes is ahead of certification/verification processes which assume hard-coding.

Embedded Systems & Pervasive Dependability

ES are "a system in which computing plays an integral but supporting role to applications that interact with the physical environment." Pervasive computing implies that ES will be prevalent in society, for example in intelligent homes and roadways. Research issues include:

- coherent collection of abstraction & techniques
- multidimensional QoS; integrated approach for handling multiple different attributes
- programming challenges
- handling changes & mobility

Survivable Subnetworks Embedded within a Critical Infrastructure

- Develop methods to model interdependencies of CI to identify the critical sub-networks
- Simulate the emergent behaviour of critical subnetworks under different attack scenarios
- How to develop metrics for prioritisation of remediation

Critical Infrastructures: Interdisciplinary Education & Research Challenges

The contemporary power industry is a complex, high-speed, high reliability machine/computer system which operates under stressed conditions. Research needs include:

- Interdisciplinary research & education
- Theoretical framework for modelling and simulation of infrastructures/interdependencies

4.3 Working Group Conclusions

The second day began with reports from the working groups. These were complemented by a reflection on "Possibilities for EU/US collaboration".

4.3.1 WG 2 conclusions

The report from the ***interdependency group*** focused on two aspects: motivations for collaboration and project suggestions.

The basis for collaboration on dependability issues was a shared vision that the future will require dependability and that global problems require global solutions. This has to be the basis for mutual understanding – between research groups from different countries as well as from different research fields – to foster community building and to enable complementarity.

To underline this, several of the suggested project options[3] are worth highlighting:

- Large scale networked embedded systems involving people (pervasive computing)
- Socio-technological issues in global computer-based systems
- Intrusion tolerant global systems (taking into account socio-technological differences)
- Global systems whose interfaces and specifications are ill-defined and/or continuously evolving
- The Grid"[4] raises major dependability issues

4.3.2 WG 1 conclusions

The ***information assurance group*** first addressed research needs and gaps, of which the following are especially noteworthy:

- Trustworthy, dynamic, complex information sharing
- Intrusion tolerance for large, dynamic ad hoc/peer-to-peer groups
- Issues arising from a framework for strong authentication and authorisation
- Developing protocols and verification techniques and new engineering capabilities

The WG identified drivers for collaboration as:

- the "insider threat"

  where inside/outside become increasingly virtual and blurred

- Applications

  Especially demanding applications including international business collaborations within a "virtual enterprise", Command & Control systems in coalition missions, or the "Computational Grid"

- Strong authentication needs

  Available technologies like PKI and biometrics stand in contrast to enterprise needs that do not want do keep (and guard) identity information

- Policy needs across several applications/user groups

[3] These are incorporated in section 3.3
[4] www.globus.org/research/papers/anatomy.pdf

Further motivations for collaboration include complementarity, the need to involve international communities of experts, improved cost-effectiveness, availability of skills and resources.

4.3.3 Plenary Discussion

The plenary discussion following the WG presentations took up the issue of information and data sharing. Here a number of questions were raised:

- What kind of data/information should be shared – e.g. data on events or incidents, data on system behaviour, data on internet traffic etc.?
- Do we want access to data of other countries, or to collect data internationally?
- Should information available to governments (such as data shared between OECD countries) be shared with research groups? with whom else?

This discussion brought out the need for international harmonisation of terms and language since much data from measurements cannot be compared due to the lack of agreed "standards", comprising terminology and protocols, both nationally and internationally.

4.3.4 Frameworks for Collaboration

The WG conclusions were complemented by a proposal for a collaborative framework. This proposal again highlighted existing collaborative successes and "lessons learned." The proposed framework for US-EU collaboration comprised:

- a minimalist steering group of US and EU participants
- stimulation of clustering and close co-operation (e.g. by staff exchanges)
- provision of technical aids

The tasks of such a framework should comprise

- Identification of suitable topics[5]
- Laying down ground rules
- Enabling joint proposals and / or participation of US in EU proposals and vice versa
- Avoidance of double jeopardy

Bureaucracy should be kept as low as possible but such a framework should support more opportunities for information exchange at the level of researchers. As an example, the EU/US project workshop in Cascais, Portugal in January 2001 was identified as good practice in stimulating information exchange and collaboration at the technical level.[6]

4.4 Other Issues

In the final section of the workshop, two initiatives were introduced:

[5] see e.g. the list of topics in chapter 3.3

[6] A copy of the identified projects and possible opportunities for information exchange was provided to all participants at Düsseldorf.

- (National) Colloquium for Information Systems Security Education
- The International Institute for Critical Infrastructures, CRIS

The National Colloquium for Information Systems Security Education will shortly be renamed the Colloquium for Information Systems Security Education to reflect the internationalisation in the field. The next Colloquium will be held 3 – 7 June 2002 in Seattle, Washington, under the title "Creating the Balance 2002 – Government, Industry, and Academia". The objective is to create an environment for information exchange between government, industry and academia as well as to provide input to the development of academic curricula. An example of the way in which collaboration on education could work would be the widespread sharing of educational material such as "best of breed" lectures between Universities.

The introduction to CRIS[7] noted that the institute was founded in January 2001. CRIS currently covers the electric power system and related communication and computer networks.

4.5 Workshop Close

The wrap-up of the workshop included overviews by the US and EU on ongoing collaborative initiatives with other partner countries or organisations.

The US is engaged in information exchange on CIP R&D issues

- on a bilateral basis with the EU and other countries world wide
- in multilateral organisations such as the APEC Forum and the OECD

Bilateral cooperation is underway between the US and Australia, Canada, UK, Mexico and Japan. On the multilateral front, it was noted that APEC has 21 members. There are 13 Working groups, of which two are related to CIP/dependability issues: the telecommunications working group (TEL) and the industrial science and technology WG (IST).

From an EU perspective, there are a number of bilateral initiatives with, e.g., the USA, Canada and Korea but no strategic policy for international cooperation. Within the OECD, the EU does not (yet) take part in the technical discussions.

Closing the workshop, US and EU representatives concluded that the events of 11 September had given added urgency to the need for collaborative R&D. The next step was to systematically pull together the threads discussed during the workshop under a steering committee that would provide a framework for joint action.

[7] se also www.cris-inst.com

Annex 1: Workshop Agenda

30 NOVEMBER 2001

19:00	**Dinner at the Restaurant:** **FISCHHAUS, Bergerstr. 3-7, Düsseldorf**

1 DECEMBER 2001

09:15	**ARRIVAL**
09.30	**WELCOME – European Commission & US Dept. of State**
09.30	**WORKSHOP AGENDA - European Commission**
09.40	**DELEGATION PRESENTATIONS AND DISCUSSION** • *State of play of the EU-USA R&D on dependability* • *Review of the EU-USA collaboration on dependability* • *R&D strategy road-mapping*
12.00	**R&D TOPICS AND DISCUSSION FORMAT** • *Dependability challenges in Information Society* • *Information Assurance of complex networked systems* • *Interdependencies*
12.30	**LUNCH BREAK**
13.30	**TECHNICAL PRESENTATIONS AND DISCUSSION** • *Dependability challenges in Information Society* • *Information Assurance of complex networked systems* • *Interdependencies*
18.00	**CONSOLIDATION OF FINDINGS**
19.30	**FINALISATION OF FINDINGS**
20.30	**END OF SESSION**

2 DECEMBER 2001

09.15	**ARRIVAL**
9.30	**PLENARY SESSION** • *R&D Collaborative Roadmap: Next Steps* • *Co-ordination mechanisms to support the Collaboration* • *Further Outreach (e.g. OECD, Japan, etc)*
12.30	**LUNCH BREAK**
13.30	**CLOSED SESSION TO DELEGATIONS AND SUPPORT STAFF** • *Preparation of the workshop summary and roadmap items*
16.30	**CLOSURE**

Annex 2: List of Presentations

Introductory remarks: Rosalie Zobel

Dec. 1, plenary:

(1) Max Lemke - "Dependability in Information Society: EU policy and technical developments"

(2) Marc LeBlanc - "Critical Infrastructure Assurance"

(3) Jay Lala - "Information Assurance Programs "

(4) Helen Gill - "US Research in High Confidence Software & Systems"

(5) Alkis Konstantellos - "EU-US Collaboration in Real-Time, Embedded and Control Systems, Status and Outlook "

(6) Rita Rodriguez - "EU-US Collaboration in Real-Time, Embedded and Control Systems, Status and Outlook"

(7) Marc Wilikens - "EU working group on Information Infrastructure Interdependencies and Vulnerabilities "

(8) Carl E. Landwehr - "NSF Trusted Computing Program "

(9) Andrew Rathmell: short note on DDSI and EWIS

(10) Frank Anger - "Information Technology Research at the National Science Foundation"

(11) David A. Jones - "Energy Infrastructure Interdependencies Program (EIIP)"

(12) Ernie Lucier - "Federal Aviation Administration (FAA), R&D in Information Assurance"

WG 1:

(1) Tom McCutcheon: Statement

(2) Ming-Yuh Huang – "Large and Complex Systems – Security Issues and Perspectives“

(3) Michael Waidner – "Dependability Challenges“

(4) William H. Sanders – "Strategy for a Dependable Information Society: Creating a Science / Engineering to Validate the Critical Information Infrastructure”

(5) Jean-Claude Laprie - "Dependability of Large, Networked Computer Systems“

WG 2:

(4) Geert Deconinck - "Open networks: how can we rely on them for control applications"

(5) Hermann Kopetz - "Research Issues in Dependable Real-Time Systems"

(6) David Sharp - "Dependability of Networked Embedded Systems"

(7) Rick Schlichting - "Embedded Systems and Pervasive Dependability"

(8) Steven Fernandez - "Survivable Subnentworks"

(9) Mark Lauby - " Critical Infrastructures: Interdisciplinary Research & Education Challenges "

(10) Brian Randell - "A Rationale for International Co-operation"

(11) Antonio Diù - "Vulnerabilities of the Electrical System as an Interdependent Infrastructure"

(12) Robin Bloomfield - "Dependability Cases - supporting collaboration and diversity?"

(13) Jacob Abraham - "Dealing with complexity in Verification and Test"

Dec. 2, plenary

(1) WG 2 Conclusions (Brian Randell)

(2) WG 1 Conclusions (Jean-Claude Laprie)

(3) Tom McCutcheon - "Possibilities for EU/US co-work identified in workgroup 1"

(4) Corey Schou - "National Colloquium for Information Systems Security Education"

(5) Hans Ottosson - "Welcome to the CRIS Institute – the international institute for critical infrastructures"

(6) Marc LeBlanc - "Critical Infrastructure Assurance"

Closing remarks: Marc LeBlanc, Rosalie Zobel

Annex 3: List of Participants

EUROPEAN PARTICIPANTS

Rosalie ZOBEL	Director **EUROPEAN COMMISSION** DG INFSO C Rue de la Loi, 200 1049 Bruxelles Belgium Tel : +32 2 296 81 68 Fax: +32 2 299 28 65 E-mail : rosalie.zobel@cec.eu.int
Michael NIEBEL	Advisor **EUROPEAN COMMISSION** DG INFSO C Rue de la Loi, 200 1049 Bruxelles Belgium Tel : +32 2 296 07 05 Fax: +32 2 296 92 29 E-mail : michael.niebel@cec.eu.int
Andrea SERVIDA	**EUROPEAN COMMISSION** DG INFSO C4 Rue de la Loi, 200 1049 Bruxelles Belgium Tel : +32 2 295 81 86 Fax: +32 2 296 83 64 E-mail : andrea.servida@cec.eu.int
Max LEMKE	**EUROPEAN COMMISSION** DG INFSO C4 Rue de la Loi, 200 1049 Bruxelles Belgium Tel : +32 2 299 15 75 Fax: +32 2 296 83 64 E-mail : max.lemke@cec.eu.int
Alkis KONSTANTELLOS	**EUROPEAN COMMISSION** DG INFSO E1 Rue de la Loi, 200 1049 Bruxelles Belgium Tel : +32 2 295 71 53 Fax: +32 2 29…. E-mail : alkis.konstantellos@cec.eu.int
Marc WILIKENS	**EUROPEAN COMMISSION** Joint Research Centre Institute for the Protection and Security of the Citizen Cybersecurity Tel: +390332 789737 Marc.Wilikens@jrc.it

Hans OTTOSSON	**CRIS – The International Institute for Critical infrastructures** EnerSearch AB SE-205 09 Malmoe Sweden Tel : +46 (40) 255000 Fax: +46 (40) 6115184 E-mail : hans.ottosson@enersearch.se
Geert DECONINCK	**K.U.LEUVEN – ESAT / ELECTA** Kasteelpark Arenberg 10 B-3001 Leuven-Heverlee Belgium tel: +32-16-32 11 26 fax: +32-16-32 19 85 e-mail: Geert.Deconinck@esat.kuleuven.ac.be
Tom McCUTCHEON	**DSTL** St. Andrews Road Malvern, Worcester, WR14 3PS UNITED KINGDOM Tel. (+44) 1684 771220 Fax. (+44) 1684 771206 Email. Tgmccutcheon@dstl.gov.uk
Brian RANDELL	**UNIVERSITY OF NEWCASTLE** Newcastle upon Tyne – UK NE1 7RU – United Kingdom Tel: +44 (191) 222 79 23 E-mail: Brian.Randell@newcastle.ac.uk
Jean-Claude LAPRIE	**LAAS – CNRS** Director 7, avenue du Colonel Roche 31077 TOULOUSE Cedex 4 FRANCE Tel: +33 (5) 61 33 62 70 E-mail: laprie@laas.fr
Antonio DIU MASFERRER	**RED ELECTRICA DE ESPANA S.A.** Paral.lel 51 08004 Barcelona Spain Tel: +34 (93) 443 08 61 Fax: +34 (93) 442 60 11 E-mail: adiu@ree.es
Hermann KOPETZ	**TECHNISCHE UNIVERSITÄT WIEN** Institut für Technische Informatik Treitlstraße 3/1821 A – 1040 VIENNE AUSTRIA Tel. (+43) 1 58801 18210 Fax. (+43) 1 569 149 Email. hk@vmars.tuwien.ac.at
Michael WAIDNER	**IBM ZURICH RESEARCH LAB** Saeumerstrasse 4 CH-8803 Rueschlikon Switzerland Tel +41-1-724 8220 Fax +41-1-724 8953 E-mail : wmi@zurich.ibm.com

Robin E. BLOOMFIELD	**ADELARD** Drysdale Building Northampton Square London EC1V 0HB UNITED KINGDOM Tel. +44 (020) 7490 9450 Fax. +44 (020) 74909451 Email. Reb@adelard.co.uk
Remi Ronchaud	**ERCIM Office** 2004, route des lucioles BP 93 cedex 06902 Sophia Antipolis FRANCE Tel: + 33 4 92 38 50 12 Fax: + 33 4 92 38 50 11 E-mail: remi.ronchaud@ercim.org

US PARTICIPANTS

Mark LEBLANC	**DEPARTMENT OF STATE** Special Advisor for CIP S&T Office of the Assistant Secretary of State for Verification and Compliance Voice: (202) 647-3517 Fax: (202) 647-1321 e-mail: LeBlancME@T.state.gov
Stan RIVELES	**DEPARTMENT OF STATE** Senior Counselor STAS Room 2819 Washington DC 20520 Tel: +1-202-647-6121 Fax: +1-202-647-6928 E-mail: RivelesSA@t.state.gov
Roy A. MAXION	**CARNEGIE MELLON UNIVERSITY** Dept. of Computer Science PITTSBURGH, PA 15213-3890 USA Tel. (+1) 412 268 7556 Fax. (+1) 412 268 5576 Email. maxion@cs.cmu.edu
Jay H. LALA	**DEFENSE ADVANCED RESEARCH PROJECTS AGENCY** Information Technology Office 3701 N. Fairfax Dr. Arlington, VA 22203-1714 Phone: (703) 696-7441 Fax: (703) 696-2204 e.mail: jlala@darpa.mil
Helen GILL	**NATIONAL SCIENCE FOUNDATION** NSF/CISE/C-CR Room 1145 4201 Wilson Blvd. Arlington, VA 22230 Phone: 703-292-8910 Fax: 703-292-9059 E-mail: hgill@nsf.gov
Carl E. LANDWEHR	**NATIONAL SCIENCE FOUNDATION** CISE/CCR Suite 1175 4201 Wilson Blvd. Arlington, VA 22230 e-mail: clandweh@nsf.gov phone: 703-292-8936 fax: 703-292-9059
Frank D. ANGER	**NATIONAL SCIENCE FOUNDATION** NSF/CISE/C-CR , Room 1145 4201 Wilson Blvd. Arlington, VA 22230 E-mail: fanger@nsf.gov

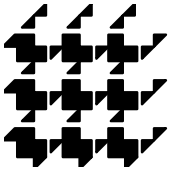
Rita V. Rodriguez	**NATIONAL SCIENCE FOUNDATION** NSF/CISE/EIA 4201 Wilson Blvd. Arlington, VA 22230 (USA) Tel +1-703-292-5188 Fax +1-703-292-9030 rrodrigu@nsf.gov
David JONES	**INFRASTRUCTURE ASSURANCE CENTER** Argonne National Laboratory 8924 Wrights Mill Road Woodstock, MD 21163 USA Tel : +1 (410) 750 3538 E-mail: djones88@rcn.com
Steven FERNANDEZ	**CRITICAL INFRASTRUCTURE PROTECTION INITIATIVE** Idaho National Engineering and Environmental Laboratory P.O. Box 1625 Mailstop 3840 Idaho Falls, ID 83415-3840 Voice 208 526 3675 Fax 208 526 4311 e-mail sfernand@inel.gov
Corey D. SCHOU	**IDAHO STATE UNIVERSITY** College of Business Campus Box 8020smi Pocatello, Idaho 83209 Tel: (208) 282-3194 Fax: (208) 282-4367 E-mail: schou@mentor.net
Ernie LUCIER	**FAA** FAA/AIO-4 800 Independence Avenue SW Washington, DC 20591 Tel: +1-202-493-5269 e-mail**:** Ernest.Lucier@faa.gov
William H. SANDERS	Department of Electrical and Computer Engineering, and Coordinated Science Laboratory **UNIVERSITY OF ILLINOIS at Urbana-Champaign** CRHC – Coordinated Science Laboratory University of Illinois 1308 W. Main St. Urbana, IL 61801 USA Tel: +1 (217) 333-0345 Fax +1 (217) 244-3359 E-mail: whs@crhc.uiuc.edu
Jacob ABRAHAM	**UNIVERSITY OF TEXAS** ACE 6.134, C8800 Austin, TX 78712-1014, USA Tel: +1 (512) 471-8983 Fax: +1 (512) 471-6967 E-mail: jaa@mail.cerc.utexas.edu
Rick SCHLICHTING	**AT&T** AT&T Shannon Laboratory, E221 180 Park Ave. Florham Park, NJ 07932 USA Tel: +1-973-360-8234 Fax: +1-973-360-8077 Email: rick@research.att.com

David SHARP	**BOEING** St. Louis, MO Tel. : +1 (314) 233-5628 Fax. : +1 (314) 233-8323 E-mail: David.Sharp@MW.Boeing.com
Ming-Yuh HUANG	Core Technology Program Manager **BOEING Phantom Works** Information Assurance and Security P. O. Box 3707, MC 7L-49 Seattle, WA 98124-2207 Tel. : +1 (425) 865-2490 e-mail : ming-yuh.huang@boeing.com
Shankar SASTRY	**University of California at Berkeley** Dept of Electrical Engineering & Computer Sciences 231 Cory hall ' 1770 Berkeley. CA 94720-1770 Tel: +1-510-642-0253 Fax: +1-510-642-2845 e-mail: sastry@eecs.berkeley.edu
Mark LAUBY	Managing Director, Operation **EPRI** 3412 Hillview Ave Palo Alto CA 94303-0813 Tel: +1-650-555-2282 Fax: +1-650-555-2929 E:mail: MLAUBY@epri.com

ORGANISATION AND TECHNICAL SUPPORT

Andrew RATHMELL	**King's College London** Strand Bridge House 138-142 Strand London WC2R 2LS Tel: +44 (0)7771 968849 Fax: +44 (0)1223 358845 E-mail: andrew.rathmell@kcl.ac.uk
Susanne JANTSCH	**IABG mbH,** Abt. IK 51 Einsteinstr. 20 D-85521 Ottobrunn Tel.: +49 89 6088 – 3167 FAX: +49 89 6088 – 2873 Email: jantsch@iabg.de
Derek LONG	**CISA Ltd** Overdale House Ashley Road – Battledown CHELTENHAM, GL52 6NU UNITED KINGDOM Tel. (+44) 1242 237 052 Fax. (+44) 1242 237 052 Email. Derek.long@cisa-ltd.co.uk
Christine SCHWARZ-HEMMERT	**IABG mbH** Abt. IK 51 Einsteinstr. 20 D-85521 Ottobrunn Tel.: +49 89 6088 – 3167 FAX: +49 89 6088 – 2873 Email: schwarz-hemmert@iabg.de
David MUSSINGTON	**RAND Corporation** RAND/STPI 1200 South Hayes St., Arlington, VA 22202-5050 Tel: (+1) 703-413-1100, x5619 FAX: (+1) 703-414-4710 Email: dmuss@rand.org

FET - Future and Emerging Technologies



DIMACS — Center for Discrete Mathematics & Theoretical Computer Science

This workshop is part of a series of strategic workshops to identify key research challenges and opportunities in Information Technology. These workshops are organised by ERCIM, the European Research Consortium for Informatics and Mathematics, and DIMACS the Center for Discrete Mathematics & Theoretical Computer Science. This initiative is supported jointly by the European Commission's Information Society Technologies Programme, Future and Emerging Technologies Activity, and the US National Science Foundation, Directorate for Computer and Information Science and Engineering.

More information about this initiative, other workshops, as well as an electronic version of this report are available on the ERCIM website at http://www.ercim.org/EU-NSF/

European Research Consortium for Informatics and Mathematics

ERCIM

www.ercim.org