Dependability
of Infrastructures
and Interdependencies

European Commission -
US National Science Foundation

Strategic Research Workshop

R&D Strategy for Sustaining an Information Society:

Dependability of Infrastructures and Interdependencies

Washington, USA,
23-24 September 2002

Workshop Report and Recommendations

EU-NSF WORKSHOP REPORT

EU-US International Workshop on R&D Strategy for Sustaining an Information Society: dependability of infrastructures and interdependencies

23-24 September 2002, Washington, USA

Report Version:	1.0
Report Preparation Date	8 May 2004
Dissemination Level:	Public

Title:	EU-US International Workshop on R&D Strategy for Sustaining an Information Society: dependability of infrastructures and interdependencies
Abstract:	The report provides a summary of the workshop discussions and conclusions
Status	Final
Date:	08 May 2004
Distribution:	Public

.

TABLE OF CONTENTS

DISCLAIMER

The workshop was organized by University of California, Berkeley, in conjunction with Vanderbilt University, the University of Virginia and the ERCIM EEIG.

Funding was provided by the National Science Foundation, with assistance from Sandia National Laboratories, and by the European Commission Future and Emerging Technologies (FET).

The workshop was held on September 23-24, 2002 at National Conference Center in Lansdowne Virginia, United States.

The workshop brought together around 60 participants from the US side with 20 dedicated EU participants.

THE OPINIONS AND VIEWS EXPRESSED IN THIS REPORT DO NOT REPRESENT THE OFFICIAL OPINIONS AND POLICIES OF THE EUROPEAN COMMISSION OR THE US DEPARTMENT OF STATE

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. Such concerns become an area of heightened awareness as national infrastructures become increasingly dependent on complex, aging computing systems which become increasingly interdependent.

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 Critical Infrastructure Protection 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 a response to the globalization of information infrastructures and services. In this globalized 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.

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 focusing on Critical Infrastructure Protection while Europe addressed the ’dependability’ areas. At Helsinki, the "Venice" recommendations were progressed by sharing information on concrete work and research programs 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.

Two further technical workshops on ’Information Assurance and Survivability’ and Attack tolerance were held at DERA Malvern (5-7 June 2000) and in Lisbon (29-30 January 2001). The aim of these workshops, which brought together researchers from a number of projects funded by DARPA and the IST Programme in the area, was to exchange experiences and results in view of facilitating some sort of closer cooperation around projects activities.

In the course of 2001, there has also been an attempt to organize a workshop on Interdependencies pooling together projects funded by DoE and the IST Programme building on the contacts established in the DOE/OSTP Workshop on "Infrastructure Interdependencies Research and Development" which took place on 12-13 June 2000 in McLean. The aim was to exchange technical solutions and practices in the area of interdependencies between the electric grid and the open telecommunication infrastructure. However, because of the electricity crisis in California (February 2001) and the 9/11 events, the workshop was cancelled twice very close to the date planned.

In December 2001, the EU/NSF D sseldorf 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. All participants agreed on the urgency to work together and internationally on RTD and technical domains related to dependability and protection of critical infrastructures and a comprehensive list of potential topics for collaboration was developed. However, in order to get a larger scale EU-US collaboration off the ground, it was agreed that a stronger effort was needed to focus and make more concrete the collaboration. To this purpose it was suggested to set up a steering group to be constituted by representatives from academia and industry in the EU and the US and be supported by the respective funding bodies.

In the US, a heightened sense of urgency and awareness of critical infrastructure protection has grown since the attacks of Sept 11. The Virginia workshop took place in conjunction with the US Technical Workshop on Information Technology for Critical Infrastructure Protection held on September 19-20, 2002. The US workshop issued recommendations for new R&D in (I) Information Assurance and Survivability, (II) Secure Networked Embedded Systems, and (III) Validated Modeling, Simulation and Visualization of Critical Infrastructure Systems and their Interdependencies. US research needs confront the issue of bring traditional approaches to Digital Control Systems and SCADA up to the standards of modern technology, and continuing long range research in information technology crucial to continuously ensuring the security of national infrastructures. This workshop followed the release of the US Draft National Strategy to Secure Cyberspace released for comment on September 18, 2002 by the Presidential Critical Infrastructure Protection Board.

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 programs 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 programs. 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 goals for the workshop were:

- to foster collaboration between the US and the EU in areas of information technology for controlling systems vital to sustaining an information society
- to examine analytical approaches to modeling the interdependencies among key sectoral infrastructures and simulating the interdependent effects of breakdowns
- to identify research priorities and establish collaboration efforts in critical infrastructure systems controlled by information technology - e.g. power systems, aviation and selected areas.

3 PROCEEDINGS

Introduction

As the primary agency for supporting fundamental, long range research, National Science Foundation and the European Commission support basic science, education, statistics gathering and other research that support science and engineering education. They also ensure that the results of research are transferred into practice in a timely manner. Both institutions actively cooperate with agencies that have direct responsibility for trust and security through sponsoring workshops and expanding horizons and opportunities that these actors have to secure the information society. The NSF and the European Commission believe in the importance of close and active collaboration at all levels.

This workshop focused on interdependencies between complex systems - on embedded systems, SCADA systems, digital control networks and systems that form foundation of Critical Infrastructures. The objective of this workshop is to focus on the long range vision to lay the foundations rather than merely fix today s problems. In the area of critical infrastructure, many of the same problems still exist that existed 30 years ago. In particular, this workshop should provide guidance for the next 5-10 years in order highlight the best approaches towards trusted and secured infrastructures.

Issues and challenges

Experts agree that there has been a frustrating lack of progress in computer security. Several reports emphasized the vulnerability of computer systems. The adoption of best practices could ameliorate the problems yet, as measures were implemented to address this issue, two deeper problems became evident:

- In most areas, there is a vigorous research base at universities. This provides a double benefit: trained people, and a set of ideas that will eventually find their way into practice. This is not true in the area of computer security, where the research base in people and ideas is tiny. Studies estimate that the US produce 7 PhDs per year in computer security (out of about 1000 PhDs in Computer Science.). This problem is also shared by Europe. Both in the EU and in the US additional research funding flowing into this area is necessary. Academics need dependable long term funding from government agencies.

- Existing security research focuses on perimeter defense. The assumption of perimeter defense - for example, firewalls, intrusion detection - is that the bad guys are on the outside and that we have to defend the stuff on the inside of the perimeter. This perspective does not work in a networked world. The model is fragile. Once the perimeter is penetrated, an intruder can run amok. The model cannot protect against inside attacks (all of the costly attacks against financial system that I know about have been from insiders).

There is also a popular misconception that security flaws are due to "bugs" — coding errors. According to an investigation done in 1993, out of the fifty studied security violation twenty-two were not due to coding bugs, but to errors in program specifications. Similarly in the area of cryptographic protocols, which are both critical and short enough to warrant formal proofs of "corrrectness", repeatedly protocols that have been proven "correct" have been broken. The problem is that the real theorem of correctness is for all values of input, nothing bad can happen . We don't have definition of what is "bad".

We can't solve the computer security problem without long-term basic research that adopts a better model than perimeter defense and recognizes that a better. Currently, this issue has the attention of policy makers, and we need to give them ideas of what can be done.

There is the potential for dratic improvements for security in cyber and physical arenas. Currently, the US and Europe are addressing their own physical and network security issues. In the future, the challenge of coordination will be greater and will call for closely coordinated efforts

In the general public, there is little awareness of new vulnerabilities, though the public is now becoming more aware. New vulnerabilities include the increasing use of DSL, cable and wireless technologies. Internet broadband has a downside of making the PC more vulnerable.

Solutions for large-scale interdependent systems will require major S&T research efforts and funding. Research establishments will need to train a much larger cadre of security people. Additionally, we will need to increase R&D beyond today s levels. However, there are limits to what the governmental institutions can contribute to solve problem when 85% of critical infrastructures are held in private hands.

Public-private partnerships are essential to find remedies to vulnerabilities. This will likely carry heavy additional cost, which the public may not accept. Customers are just beginning to recognize the need for security, and customers must *see* the value of greater security.

Interdependency analysis is being approached on each side of the Atlantic. National infrastructures are more tightly coupled. We do not yet have comprehensive understanding of the complicated interdependency issues. Further, there is an artificial divide between physical and cyber- security. This situation is improving under reevaluation since 9-11. There has been more research modeling complex interdependencies, analyzing cascading failures, identifying vulnerabilities. We hope this will lead to solutions resting on solid foundations in science and technology. The mission to solve these problems will only be fulfilled by investment in R&D and increased engagement of the S&T community.

There has been significant movement and development in this area. There exists a sense of urgency to address cybersecurity, coupled with an understanding of the devastating economic consequences we face if we do not address this issue.

EU/US workshop presented talks

Hereafter are several of the presentations given during the workshop. Additional speakers have participated to the event. The full list of participants in to be found in annex.

Cita M. Furlani, NCO ITR&D Cross Agency Program

Dr. Furlani discussed NITRD program coordination and reviewed agency NITRD budgets for FY2003. There is a need to establish priorities regarding the technical issues associated with physical and cyber infrastructure and define the priorities are for Critical Infrastructure Protection technologies and international collaboration. Since we cannot address every vulnerability in our efforts to secure national infrastructure, the NITRD office requests guidance on where to focus resources.

Doug Schmidt, DARPA IXO

Distributed applications are growing more interconnected and internetworked, and are also relying increasingly on commercial-off-the-shelf (COTS) hardware and software that contains security flaws, both known and unknown. A new approach to this problem is derived from the concepts of providing a layered defense against intrusions, while continuing to provide varying degrees of service despite the ongoing intrusion. Important R&D efforts are focusing on developing, demonstrating, and deploying a set of middleware-based technologies that allow mission-critical distributed software applications to resist many forms of malicious intrusions. These middleware technologies manage end-to-end application quality of service (QoS) to enable more agile applications that can adapt to work around the effect of attacks, thereby offering more dependable service, and minimizing the gain from inevitable intrusions.

Ernie Lucier — Federal Aviation Administration

Many FAA systems are being replaced and/or upgraded. For example, Federal Aviation Administration telecommunications are transitioning to TCP/IP, we are developing a digital air-to-ground communication system (i.e., Controller to Pilot Data Link Communications (CPDLC)), and wireless, while not yet used, will probably be part of the future FAA. Every new technology brings new risks and a need for new security.

FAA systems have some unique characteristics. FAA is one of the 187 countries that make up the aviation community in the International Civil Aviation Organization (ICAO). A major characteristic that sets the FAA apart from other U.S. Government organizations is all systems are open and detailed information and equipments are available to anyone that wants to purchase them. As a result, FAA stresses integrity and availability (i.e., mission survivability) more than confidentiality in its systems. FAA security policy requires a protection profile to document these priorities for all new systems. To facilitate the protection profile the FAA has recently developed a National Airspace System (NAS) Protection Profile (PP) Template and Supplement (e.g., applying the Common Criteria to systems) for systems of systems (as opposed to individual equipment components. (The National Institute of Standards and Technology (NIST) is using the FAA PP as a starting point for a government wide NIST Protection Profile Template.)

The FAA must rely on other agencies for R&D in Information Technology (IT) and Information Systems Security (ISS) and accept industry products developed for industry and other agencies. This is because the FAA is an operational agency and has a small R&D budget (i.e. less than 1%) compared to agencies whose mission includes research and there is no allocation for IT and ISS. To accomplish our goals in IT and ISS the FAA leverages the efforts of other agencies by providing minimal supplemental funding to transition R&D products to the FAA environment.

Carl Landwehr, National Science Foundation
Trusted Computing Program: Background and Directions

Carl Landwehr provided an overview of NSF's Trusted Computing program, a new basic research program intended to build US academic research capability in this vital area. The initial program announcement drew approximately 130 proposals, a relatively large number for NSF programs of this size ($5M per year), of which approximately 30 were funded. Roughly 85% of the grants focus on improving the foundations for the next generation of cyber infrastructure; the other 15% aims to strengthen the current environment. Dr. Landwehr also discussed related programs within NSF and the Infosec Research Council, which provides informal coordination of related research activities throughout the US government.

Sam Varnado, Sandia National Laboratories, National Infrastructure Simulation and Analysis Center (NISAC)

The US infrastructure is very difficult to protect because of its size and complexity. Further, the infrastructure is being more interdependent, i.e., banking and finance depend upon telecommunications, which depends on electric power, which depends on water, and so on. This leads to cascading failures where a failure in one infrastructure segment can cause failures in the rest of the infrastructure. Protection is complicated by these interdependencies, because they make it difficult to identify critical nodes and they can amplify the consequences of failures. The infrastructure is a complex system of systems whose behavior is difficult to predict.

Current attempts to understand the operation of the infrastructure and its vulnerabilities are stove-piped by infrastructure element, e.g., electric power. Sandia and Los Alamos National Labs have established the National Infrastructure Simulation and Analysis Center (NISAC) to provide the modeling and simulation required to understand the interdependencies among the US infrastructure elements.

NISAC will capitalize on previous investments made by the two labs in developing infrastructure models. In addition, the availability of the world s fastest computers at these labs will provide the technical capability to produce very high resolution models of various infrastructure features as needed. The ultimate goal is to be able to identify critical nodes, predict the consequences of outages, and design optimal protection and mitigation strategies for the key elements in the US infrastructure. NISAC uses a consequence based, rather than a threat based approach, to infrastructure analysis. Results from this effort will support policy makers in making decisions about infrastructures and will provide for education and training of first responders, and provide real-time crisis support.

A variety of models will be needed to accomplish the NISAC mission. These models range from simple indications and warnings models that are based on spread sheets, to agent based models to high resolution simulations using population dynamics, such as the Los Alamos transportation model called Transims.

While Sandia and Los Alamos are the core partners for these activities, they are looking for additional university, national lab, and private industry partners so that the new Department of Homeland Security has access to the best modeling and simulation capability in the nation. Argonne National Laboratories, and four universities have already been added to team.

Ian Hiskens University of Wisconsin,
Modeling and Analysis of Multilayer Interactions in Electrical Systems Vian onlinear Time Delays,

Nonlinear time delays provide an important link between the various layers of power systems. A postulated scenario of multilayer interactions, ultimately leading to cascading failure, was presented. The basic steps in this scenario consisted of an initiating overload event leading to market disruption. The associated increased market activity could lead to greater delays in the communication system, adversely affecting SCADA system response, and retarding automatic generation control. This in turn would result in further overloads, and cascading failure. To capture such a scenario, models need to include continuous dynamics, discrete event, and nonlinear time-delays. A systematic modeling approach would facilitate algorithms for addressing parameter estimation, boundary value problems, and optimal control.

Reinhard Hutter IABG, D
The European Project ACIP

The current EU roadmap project ACIP focuses on Analysis and Assessment for Critical Infrastructure Protection . It lays out the rationale why many open questions and problems in the area of concern will most efficiently be treated by the use of modeling and simulation (M&S) techniques. The study will propose:

a) a roadmap for developing a comprehensive M&S architecture ranging from technical level up to strategic planning and decision support level, and

b) ways of how to apply these tools to the different problem domains of CIP, including planning support, system design optimization, operations monitoring, early warning and response, decision support, economic evaluation of investments into security (LCC and RoI) vulnerability and sensitivity analyses, assessment of protection and reaction strategies and many more.
The change of paradigms, when compared to the classical military OR type analyses poses a great challenge to the analytical community as well as to the infrastructure stakeholders. They include multi-disciplinarily, asymmetric and multi-sided scenarios, highly dynamic behavior and complexity of systems, interdependencies within systems of systems, variable, sometimes even contradicting MoEs (e.g. between the public and the private sector).

This altogether requires new analytical approaches. Limited time and budgets will suggest to demand focus and prioritization, use of commercially available tools (e.g. POWERSIM), and borrowing ideas and approaches from other disciplines like Physics, Bio-Immunology, AI or Genomic Sciences.

There are many parallels and similarities in the related work being performed in the US and in the EU, respectively.

Antonio Diu, Red Electrica
Modeling of Different Power Transmission Systems Infrastructures (Problems and Solutions) and Their Intra-dependency, including the Natural Expansion to Include and Analyze Other Infrastructures (Telecom, Internet, Transport)

Red Electric has approached modeling critical infrastructures through mathematical modeling of networks. The model introduces contingencies to analyze outcomes in systems with strong interdependencies. It is not sufficient to base a model on one country, as neighboring countries must be taken into consideration. This ensures preparation of scenarios to expand contingencies to multiple infrastructures. This complex system modeling can be applied in different levels of details, including scenario generation and system observation. This is immensely useful for complex contingency analysis, test defense plans and provide training.

Sandro Bologna, ENEA
Linking Complex Systems and Interacting Agents Approaches for Modeling and Simulation of Critical Infrastructures and their Interdependencies

Large Complex Critical Infrastructures are inherently difficult to understand and modeling for the following reasons: structural complexity, network evolution, connection diversity, node diversity, dynamical complexity. If we now couple many such systems together, what can be said about their collective dynamic behaviour?

Currently, there are no mathematical models that can create useful top-down models for LCCIs systems, that is, models that start from large-scale graphs, systematically map them into de-coupled sub-systems, and investigate the interactions between them. Because there are so many components and potential interactions, deriving all-encompassing rules for complex infrastructures is impractical.

An alternative would be developing a bottom-up approach using autonomous adaptive agents, which allows implementation for the individual parts of a system. By concentrating on smaller parts of the system, deriving rules becomes more practical. Bottom-up models based on autonomous adaptive agents let us evaluate the local mechanisms that produce emergent patterns at system level. Emerging Agent-Based Modeling (ABM) focus on the individual parts of a system rather than the whole; focusing on smaller parts of the system makes deriving rules more practical.

Recently, the growing interest in complex systems has prompted the study of real networks with novel and previously uncharacterized topological properties. What we need is to define a unifying framework, which can be fundamental in order to fully develop a solid theoretical understanding of the physical processes underlying the formation of complex networks. This has to be done in a fully interdisciplinary perspective, through the exchange of experiences in the diverse fields of expertise of a wide scientific community for which complex networks is a useful working tool.

Recent progresses in this area have shown that most probably a single law governs the behavior of the proteins in our body, the Internet, a cool collection of atoms and sexual networks. All of them are complex networks that can be represented by the same model that capture the key properties of them. They have a lot of nodes with a few links, a few nodes with a medium number of links and a very few nodes with loads of connections. If you plot these numbers on a graph, you end up with an ever-decreasing curve characteristic of what physicist call a power law.

A new term as been invented to distinguish this type of networks from random graphs; they are normally reported as scale-free network.

Eyal Adar, iTcon
Analysis of Practicality of Models and Tools

Eyal Adar, CEO of iTcon (IT Consultants, a firm of security architects) spoke about the need for the introduction of practicality to the models and tools used in CIP. The current methodologies in the information security area come from two sources. One is high level methods (e.g. Common Criteria, BS7799) - models that are very helpful and advanced but were built to last and therefore do not include practical knowledge (e.g. specific vulnerabilities, detailed actual architecture of systems). The other source of information is the product-driven knowledge. This knowledge is highly dependent on actual products and their evolution and does not amount to security models. Eyal showed the need to bridge both extremes by introducing practical methods for security architects who face the challenge of designing large critical systems, and offered several parameters that will help the process if they become part of the models. The parameters: Ready to use, templates for specific scenarios, the ability to integrate detailed technical information, existence of set of tools for implementation, are all essential in constructing a comprehensive and practical approach to CIP.

Gwendal Le Grand, ENST
Methodologies and requirements to model and investigate criticality, vulnerability, interdependency, design-measures of critical infrastructures on a technical level

The work presented was realized in the context of the IST ACIP project in which we study available methodologies and requirements to model and investigate criticality, vulnerability, interdependency, and design measures of critical infrastructures on a technical level. A state of the art in CIS investigations was executed in order to design new security models for critical infrastructures with special emphasis on disruption impacts, and cascading effects. The main goals to be achieved are prevention, detection, identification and recovery.

From these studies, it appears that large infrastructures are different than classical systems. They can be represented by an abstract morphology characterized by three components: communication (the system coupling with the environment -- laws of physics, syntax, semantics), connectivity (the system's internal morphology -- for example a bus or a point to point architecture), and infiltration (the coupling with the system -- mimesis or camouflage). Specific security policies can then be derived from the abstract morphology.

In the case of big aggregated systems, abstract morphologies provide a means to assess the vulnerability of the system. But in order to achieve this, a better feedback from the users and infrastructure operators is needed.

4. HIGHTLIGHT SESSIONS

1. MODELING AND SIMULATION OF CRITICAL INFRASTRUCTURES AND THEIR INTERDEPENDENCIES

EU CO-CHAIR: MAX LEMKE
US CO-CHAIR: SAM VARNADO

The Working Group on Modeling and Simulation concluded to pave the way for future transatlantic co-operation. A co-operative effort will most certainly

- avoid duplication of work on either side
- cross-fertilize analysts and researchers on either side, this way, and
- contributing to a much more cost effective and efficient way of analyzing Critical Infrastructure Orotection problems

It was agreed, that a two step approach should be taken in order to prepare future co-operations.

Step 1 A management type meeting to identify objectives, chances, obstacles of establishing co-operation, and to show options for the way ahead

Step 2 Supposed a positive outcome of Step 1, a follow-on meeting of experts should identify the most promising (maybe also most urgent) fields of technical cooperation in the sense of building synergies and promote the efforts on both sides.

The following Point of Contacts were nominated:

- Sam Varnado, NISAC, Sandia Lab, Albuquerque, and

- Reinhard Hutter, IABG, Munich.

They were tasked to arrange the meeting according to Step 1 (above) in early 2003.

2. INFRASTRUCTURE INTERDEPENDENCIES: TECHNOLOGIES

EU CO-CHAIR: ANDREA SERVIDA
US CO-CHAIR: HELEN GILL

This session involved speakers from both Europe and the Unites States. Among the different talks given by the guest participants are the following:

Henk Blom, NLR

Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design - HYBRIDGE Project

Henk Blom from NLR (Amsterdam) presented the main theme of the project HYBRIDGE that is being conducted for the European Commission (EC) by a consortium of several European partners. The 21st century finds Europe and the USA facing a number of remarkable changes, many of which involve large complex real-time systems. The management and control of these systems undergoes a natural trend of becoming more and more distributed. At the same time, the safety criticality of these systems tends to increase. However good the control design for these systems will be, humans are the only ones carrying responsibility for the operational safety. This implies a need to embed the analysis and design of control and management systems for safety critical operations within sound a safety management approach such that safety levels remain well under control of the humans that carry the responsibility. The objective of HYBRIDGE is to study this issue and has selected Air Traffic Management as the most challenging illustrative application for this. More information is on the web site http://www.nlr.nl/public/hosted-sites/hybridge/.

Prof N. HadjSa d and Prof Yves Brunet, INP Grenoble/LEG, France

The Role of Distributed Resources in the Mitigation of the Vulnerability of Critical Infrastructures

Yves Brunet gave a presentation of the work made at INP Grenoble on the role of distributed resources to reduce the vulnerability of Electrical Energy Infrastructures. The event of deregulation, the pushing to the limits policy and the emergence of new technologies give a chance to distributed generation.˚Reliability and security are essential points, especially during critical conditions and recent failures of the French power system during severe atmospheric conditions triggered the attention of French authorities on vulnerability problems in Electrical Systems. RTE, the new french transmission system operator, has drawn the lessons of these events, and distributed generation may be a part of the solution to mitigate the vulnerability of electrical infrastructure. Nevertheless, the success of the interconnection of small, dispersed generation devices depends on other technologies such as ICT. We have to solve the stability problems of interdependant distant parts of an electrical network, using for exemple Phasor Measurements Units and Remote Feedback Controllers through a Global Positioning System. This is only useful when you are sure to dispose of secure communication networks and precise and real-time response measurements. These researches are explored in a basic public research lab (LEG) and a new structure mixing public and private funds (EdF, Schneider), dedicated to more applicative research (GIE). The lab is involved in national and international collaborations and the 6th European Framework Program will be for us a good apportunity to develop this activity where collaboration is an important issue to solve interdependancies of critical structures.

Brian Randell, University of Newcastle
ISDI and the Future of Dependability Research in EU

Brian Randell, of the University of Newcastle upon Tyne, gave an overview of the EU-funded "Accompanying Measure" on System Dependability (AMSD). This is of one year's duration, and is being undertaken in cooperation with four partner organizations, namely Adelard (UK), CNUCE - Univ. of Pisa (Italy), the EU Joint Research Centre (Italy), and CNRS-LAAS (France). Its activities form part of the preparations for the EU Framework 6 Information Society Technologies (IST) Programme. Specifically AMSD is undertaking two "road-mapping" exercises, one on dependable embedded systems, the other taking a holistic view of dependability by bringing together the results of a number of road-maps, e.g. on mobile privacy & security, critical infrastructure protection, smart cards, cryptography, dependable embedded systems, etc.

This latter overall roadmap aims to cover both technical and socio-technical issues, and a broad range of systems. Material from all the more-focused roadmaps will be consolidated, so as to identify commonalities, tensions, and contradictions (as well as opportunities for synergy) using the taxonomies and classifications of dependability developed by IFIP WG 10.4 (Dependability and Fault Tolerance) as the conceptual framework. As a contribution to this activity, and as a part of a major community and consensus building exercise, a number of joint workshops are being held. The hope is that as a result of these various activities the IST Programme will include a coherent set of well-aimed major projects encompassing a full range of dependability-related activities, e.g. R&D on the various aspects of dependability per se, (reliability, safety, security, survivability, etc.); education and training; and means for encouraging the use of dependability best practice.

Matthias Schunter, IBM
Dependability and Privacy - Can auditing and privacy co-exist?

The talk "Dependability and Privacy" first recalled the four major strategic challenges for dependability. These are intrusion tolerance for large, dynamic, ad-hoc and peer-to-peer groups, self-improving systems, application-level intrusion detection, and methodologies for sound security engineering when designing and building systems.

The second part of the talk defined privacy to be the right of individuals to determine what data is collected for what purpose. A distinguishing feature is that once privacy is lost, recovering is difficult if not impossible.

As a consequence, privacy must be built-in and supported from the beginning. One basic paradigm for building privacy-protecting systems are to collect all data where the link to the actual identity of a customer is not important under so-called pseudonyms. Another basic paradigm is data-scarcity, i.e., to collect and store only the data that is actually needed and to collect it in the least privacy invasive type (anonymized vs. pseudonymized vs. personal).

Besides building privacy-protecting systems, an important aspect is the maintenance of trust into the running systems. This can be done by open design, third party & open security evaluation and by enabling users to freely decide whom to trust.

Paulo Verissimo, University of Lisbon
Distributed Computing and Infrastructure Interdependencies

Paulo Ver ssimo, from the Univ. of Lisboa Faculty of Sciences, Portugal, gave a talk representing Maftia/CaberNet activities concerning Distributed Computing Infrastructure Interdependencies.

The CaberNet Infrastructure Technology was briefly reviewed, as an example of a research-supporting infrastructure, and thus with less concern for criticality: Common fail-safe NoEs entry portal; Coherent replicated File + Web servers; Global file system updates; Web-all-over; Best-server lookup; Guest Pages Service ; NSI-lite service; Server updating service; LDAP service. MAFTIA - Malicious and Accidental Fault Tolerance for Internet Applications, is an IST project under the umbrella of CaberNet. The main objectives are: Architectural framework and conceptual model for IT; Mechanisms and protocols-dependable middleware; large scale intrusion detection systems; dependable trusted third parties; distributed authorization mechanisms; Validation and assessment techniques.

Partners are: DERA/Qinetiq, Malvern (UK),IBM, Zurich (CH), LAAS-CNRS, Toulouse (F), Newcastle University (UK)(Coord.), Universitaat des Saarlandes (D), Universidade de Lisboa (P). EU coordinator: Andrea Servida. An overview was made of the MAFTIA Architecture building blocks, and of the main application support blocks: IT Transactions with Error Masking, IT Authorisation Service, IT Intrusion Detection Service.

Relevant pointers:

- Navigators Group at the Univ. Lisboa, Portugal http://www.navigators.di.fc.ul.pt
- CaberNet site: http://www.research.ec.org/cabernet
- MAFTIA site: http://www.research.ec.org/maftia

David Nicol, Dartmouth College
Simulation Technology for Large-Scale Infrastructure Dependency Analysis

Key research issues in the analysis of critical infrastructure dependencies revolve around coordinated representation of different systems, the representation of known interdependencies, and the discovery and analysis of additional dependencies. A great deal of computational effort will be required to conduct this analysis, and will certainly involved simulation. For this effort to be successful, it will be important to consider low-level systems issues when designing the analysis tools. The key issues are modeling methodology, model representation (e.g. databases), automated assistance of experimental design and output analysis, mixed analysis modes, and implementation on large-scale parallel computing platforms.

Rajeev Raje, Indiana University Purdue University Indianapolis, and Barrett Bryant, University of Alabama at Birmingham
UniFrame: A Framework for Seamless Interoperation of Heterogeneous Distributed Software Components

Rajeev Raje from Indiana University Purdue University Indianapolis gave an overview of the UniFrame project. UniFrame is supported by the DoD and ONR under the Critical Infrastructure Protection/Software program.

UniFrame aims at creating a seamless framework for interoperation of heterogeneous software components. Many challenges need to be addressed while creating such a framework.

These include, the discovery of components, the assurance of the quality of service (QoS) offered by the components, the semi-automatic generation of the glues and wrappers for interoperation, the composition and decomposition models for the quality of service parameters, the creation of the necessary tools for integration and validation the system made up of components and an appropriate usage of the formalism during the entire process.

Many critical systems have stringent requirements for various QoS attributes. The software for these systems is generally hand-crafted, thereby, increasing the chances of failures and insertion of errors. Hence, automation is needed (to the extent feasible) that can assist in achieving and validating a composition of components, each delivering a promised QoS. UniFrame is addressing many QoS-related issues, solutions to which, will have an impact on the creation of QoS-aware distributed software systems.

Chika Nwankpa, Drexel University
Information Embedded Power Systems: Problems and Opportunities for this Critical Infrastructure

In this talk Chika Nwankpa advocated the need for the development of a model of and electrical power systems, with its inherent embedded communication system, for the purpose of studying the characteristics of power system measurement errors due to communication delays. This model is referred to as an "information embedded power system" to emphasize the inclusion of information variables that represent measurements that have been delivered across the communication system and observed at a control center. These information variables are added to the standard power system model for the energy balance within the power system.

The reasons for this study are:

- Deregulation has motivated utilities to use tools that require accurate real-time network functions
- Faster telecommunication systems are needed in order to support these real-time network functions in energy management systems
- Little research has been performed to analyze how measurement delays can affect the accuracy of power system measurements

Chika Nwankpa also advocated the need for an experimental platforms to validate the developed model.

Bruce McMillin, University of Missouri-Rolla
Trustworthy Object-Oriented Distributed Embedded Hybrid Systems

Bruce McMillin from the University of Missouri-Rolla (UMR) gave an overview of using object-oriented methods effectively to achieve fault tolerance and security for embedded hybrid manufacturing and power systems (EHS). Typically, engineering software development is done by separating software into functions that interact in control loops with hardware often resulting in brittle software. UMR computer scientists work closely with manufacturing and power engineers to develop object models that put all components of an EHS on a common semantic framework to improve robustness and reusability.

The problem with this can be that unconstrained object oriented implementations lead to numeric inefficiencies. UMR is developing static polymorphism techniques that alleviate these inefficiencies. Fault tolerance and security of the resulting system is of major concern. UMR has developed wrapper technologies that evaluate and ensure correctness of the distributed components of an EHS. The object model is attractive for wrappers due to the encapsulation provided by objects; temporal logic expressions can be evaluated over global state properties at object interfaces. UMR is implementing these concepts on a laser-deposition milling machine and on a FACTS controlled power system. This work will help reduce the societal barriers to object-oriented implementation of engineering applications and provide for improved performance, security, and fault tolerance of hybrid embedded systems.

Yigal Arens, USC/ISI
Technology and Policy in Support of Recovery from Unexpected Events

One of the most vexing characteristics of events like those of September 11 is that they are completely unexpected. It is not simply that their precise nature or timing comes as a surprise; such events fall entirely outside the range of the planned capabilities of the organizations tasked to deal with them. Responding to them calls for resources beyond those previously allocated.

Authorities typically find themselves struggling not just with the consequences of the catastrophic events, but also with the problem of obtaining timely information about unfolding events. Background information about the environment, available personnel and other resources is often unavailable, and planning and coordinating a response in such uncertain and rapidly changing circumstances is extremely difficult. Furthermore, trying to act in this ill-defined environment can leave the authorities and society exposed to additional attacks.

While it may appear on the surface paradoxical to attempt to prepare for the unexpected , the current state of information technology makes it possible to create a general infrastructure and develop general capabilities that can be adapted instantly to react to any threat. Society cannot afford to prepare for every eventuality, but it is possible to create a foundation upon which a response can be constructed quickly.

In his talk, Yigal Arens of the Information Sciences Institute of the University of Southern California discussed a workshop he directed with Paul Rosenbloom, also from USC/ISI, in February 2002 for the NSF. Among other matters, the workshop brought out technology and policy issues that need to be addressed to better enable society to respond to unexpected disastrous events.

Phil McKinley, Michigan State University
RAPIDware: Design of Adaptive Software for Always-On Systems

Philip McKinley of Michigan State University presented an overview of the RAPIDware project, which is supported by the ONR Critical Infrastructure Protection and Adaptable Software Program.° RAPIDware addresses the design of adaptive middleware to support distributed applications in heterogeneous environments.° Targets systems include those that must continue to operate correctly during exceptional situations, such as systems used to control electric power grids, telecommunication networks, nuclear facilities, and command and control infrastructures. Such systems require run-time adaptation, including the ability to modify and replace components, in order to survive hardware component failures, network outages, and security attacks.°

A major goal of the RAPIDware project is to develop a unified software framework for adaptability that enables dynamic composition of middleware services while preserving functional and nonfunctional properties of the system. Presently, the

RAPIDware group is investigating programming language support for run-time adaptability through computational reflection and aspect-oriented programming.° Early results include an extension to the Java programming language, referred to as Adaptive Java, and its use in providing adaptability in mobile computing environments.

David E. Bakken, Washington State University
GridStat Middleware for More Extensible and Resilient Status Dissemination for the Electric Power Grid

David Bakken from Washington State University (WSU) gave an overview of GridStat, WSU's extensible middleware for providing status information to participants in the electric power grid. The communication system for the US's electric power grid was designed decades ago based on the existence of single, vertically-integrated utilities needs. It is hardwired, dedicated, and slow, and today many things are hard-coded based on this infrastructure: application programs, status information, control decisions, etc. However, the combination of deregulation of generation is creating many more participants needing status information involved in many more ways then was envisioned when the grid's communication system was designed.

Additionally, there are many more intelligent devices providing status information in many more ways. GridStat is middleware being designed and developed at WSU to provide flexible status dissemination. It provides a simple publish-subscribe model for status dissemination where subscribers are provided a cached value of each status item. GridStat's hierarchical management system manages a network of internal store-and-forward servers that optimize for the semantics of status items and provide quality of service in terms of timeliness, redundancy, and (soon) security.

Joseph Cross, Lockheed Martin
CIP Issues Relevant to Military Avionics

Joe Cross from Lockheed Martin defined the domain of military avionics as comprising the hardware and software that provides mission-critical but not flight-critical functions in military aircraft. The threats to avionics systems that impinge from outside the aircraft, such as communications jamming and spoofing, and well understood and well defended against. Threats that arise from inside the aircraft, such as subverted software and firmware, are less well understood and less well defended. Several approaches are available for addressing this internal threat, including code auditing tools, and the use of the OMG's (Object Management Group) MDA (Model Driven Architecture) approach combined with model-checking technologies.

Lamine Mili, Virginia Tech
International Institute for Critical Infrastructure

Lamine Mili from Virginia Tech presented the objectives and research activities of the International Institute of Critical National Infrastructures. The founding members of this institute, referred to as CRIS, are Virginia Tech (USA), Institute Nationale Polytechnique de Grenoble (France), the University of Hong Kong and Hong Kong Polytechnic (Hong Kong), EnerSearch (Sweden), and Ecole Polytechnique Federale de Lausanne (Switzerland). These are six world-class organizations dedicated to research and developments in the electric power, communications, and computer areas.

These complex networked systems are increasingly interdependent on each other as the digital society mature at a global scale. Consequently, their vulnerability and security are raising major concerns worldwide. This is the reason why CRIS has put forward as one of its main objectives the development of risk-based methods and technologies that will make these critical infrastructures resilient to natural and man-made catastrophes. Natural disasters include earthquakes, hurricanes, avalanches, floods, fires while man-made disasters consist of wars, insurrections, riots, and sabotages. A typical example of a critical infrastructure vulnerability that undergoes a rising vulnerability to catastrophic failure is the electric power transmission network.

Aloysius K. Mok, The University of Texas at Austin
Dependable Real-Time Embedded Systems

Dependable computing systems require not one technology but the synthesis of three types of computer system design technology: fault tolerant computing, real-time computing and secure systems technology. Because we must anticipate penetration and damage to our systems, we need a synthesis of technologies to enable systems to adapt to changes in the operating environment and to do so in real time, in a secure manner.

To this end, we introduce novel concepts about virtualizing resources in a way to preserve timeliness properties in applications and to enforce isolation between application components. This is realized in the concept of RTVR (Real Time Virtual Resource), which has nice mathematical properties and is readily implementable using COTS technology. We also discuss monitoring resource usage by a combination of design-time verification and run-time active monitoring in the TINMAN security architecture and end with speculations on the intriguing issue of imparting "free will" to real-time adaptive agents.

Annexes

Annex 1: Workshop Agenda

Annex 2: List of Participants

Annex 3: Context and Reports from related US and EU workshops

Annex 1: Workshop Agenda

MONDAY, SEPTEMBER 23RD , 2002

9:00-9:15 Introduction

Dr. Peter Freeman, Assistant Director of CISE at NSF

9:15-9:45 Keynote: The US National Academies' Counter-terrorism Activities

Dr. William A. Wulf, President, National Academy of Engineering

9:45-10:00 US Perspective On International Collaboration In S&T

Dr. Norm Neureiter, Science and Technology Adviser to the Secretary, D. of State

10:00-10:15 EU Overview Of Current Collaboration Efforts In Dependability And The EU 6th Framework Programme (FP6): New Instruments For Research

Alessandro Damiani, and Andrea Servida, EC

10:15-10:30 Critical Infrastructure Protection and NS/EP

Mark LeBlanc, Senior Policy Advisor, OSTP

10:45-11:30 ROUND-TABLE ON AGENCY ACTIVITIES

- Defining The Context For IST In FP6: ISTAG And IRG Reports

Andrea Servida, and Alessandro Damiani, S&T Advisor

-Organizing The Transition To FP6: Roadmap Projects In Security & Dependability

Max Lemke, EC

- US Programs - Roundtable

- Cita Furlani/Sally Howe, NCO
- Cyberinfrastructure report,
- ITRD actions related to CIP
- Helen Gill, High Confidence Systems and Software
- DARPA (Doug Maughan, John Bay, Doug Schmidt)
- FAA (Ernest Lucier)
- ONR (Ralph Wachter, Geoffrey Main)

- NSF (Helen Gill, Priscilla Nelson / Miriam Heller, Carl Landwehr, James Momoh, Frank Anger, Larry Brandt / Valerie Gregg)

11:30 — 12:00CONTEXT AND REPORTS FROM RELATED US AND EU WORKSHOPS

11:30-11:45 EU Workshop European Requirements for Research and Development in Information Infrastructure Dependability - (September 2002)

Andrew Rathmell King s College, UK; Reinhard Hutter IABG, D

11:45-12:00 Report of US workshop on Innovative Information Technologies for Critical Infrastructure Protection

Dr. Shankar Sastry, UC Berkeley, and Dr. Janos Sztipanovits, Vanderbilt University

1:00-1:30 Homeland Security Act

Dr. Sam Varnado, Director of Information and Infrastructure Systems, Sandia National Laboratories

01:30—03:15 MODELING & SIMULATION OF CRITICAL INFRASTRUCTURES AND THEIR INTERDEPENDENCIES
(EU co-chair: Max Lemke, US co-chair: Sam Varnado)

EU Contributions:

Analysis & Assessment for Critical Infrastructure Protection - overview of the European ACIP project, Reinhard Hutter, IABG, D

The German Cyber Terror Exercise CYTEX: macroscopic modeling and simulation of the major critical infrastructures and their interdependencies Reinhard Hutter, IABG, D

Modeling of different power transmission systems infrastructures (problems and solutions) and their intra-dependency, including the natural expansion to include and analyze other infrastructures (telecom, internet, transport,...) Antonio Diu, REE, E

Information- and communication technology-induced risks for critical infrastructures Paul Friessem, Fraunhofer SIT, D

Linking Complex Systems and Interacting Agents approaches for modeling and simulation of Critical Infrastructures and their Interdependencies Sandro Bologna, ENEA, I

Methodologies and requirements to model and investigate criticality, vulnerability, interdependency, design-measures of critical infrastructures on a technical level Gwendal.Legrand, ENST, F°;

Analysis of practicality of models and tools , Eyal Adar, Itcon, ISR

US Contributions:

National Infrastructure Simulation and Analysis Center (NISAC), Sam Varnado, Sandia National Laboratories

Risk Analysis, Jacov Haimes, University of Virginia

Risk Management and Communication, Jack Harrald, George Washington University

Model-Based Design of Complex Systems, Janos Sztipanovits, Vanderbilt University

New Systems Science, Shankar Sastry, UC Berkeley

Modeling and Analysis of Multilayer Interactions in Electrical Systems Via Nonlinear Time Delays, Ian Hiskens, University of Wisconsin

Dynamic Modeling of Infrastructure Interdependencies, Linda Nozick, Cornell University

03:30-04:00 DISCUSSION

04:00 — 5:00 INFRASTRUCTURE INTERDEPENDENCIES: TECHNOLOGIES (EU co-chair: Andrea Servida, US co-chair: Helen Gill)

EU Contributions:

ISDI and future of dependability research in EU - Brian Randell, University of Newcastle

Infrastructure dependability and privacy concerns - Matthias Schunter, IBM

Distributed computing and infrastructure interdependencies - Paulo Verissimo, University of Lisbon

US Contributions:

NSF/DARPA research in Distributed Real-time Embedded Systems, Doug Schmidt, DARPA

Simulation Technology for Large-Scale Infrastructure Dependency Analysis, David Nicol, Dartmouth

UniFrame: A Framework for Seamless Interoperation of Heterogeneous Distributed Software Components, Rajeev Raje, Indiana University Purdue University Indianapolis, and Barrett Bryant, University of Alabama at Birmingham

TUESDAY, SEPTEMBER 24th , 2002

- **09:00 — 11:30 INFRASTRUCTURE INTERDEPENDENCIES: TECHNOLOGIES**
  EU Contributions:

- The Role of Distributed Resources in the Mitigation of the Vulnerability of Critical Infrastructures — Yves Brunet, LaboratoireElectrotechnique de Grenoble
- Experimentation of a Monitoring and control system for managing vulnerabilities of the European Infrastructure for Electrical power exchange - Antonio Diu, REE
- Some research problems on dependable complex interconnected systems - Luca Simoncini, CNUCE
- Avionics system development environments to meet high dependability needs for embedded control systems for avionics - Werner Damm, OFFIS
- DDSI Project: lessons learnt on interdependencies and early warning - Andrew Rathmell, King s College
- The loss prevention approach: WG-ALPINE Project - David M. Lounsbury, The Open Group
- Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design - HYBRIDGE Project - Henk Blom, NLR
- Current and emerging trends in UK dependability research, A government perspective -Tom McCutcheon, DSTL

US Contributions:

- International Institute for Critical Infrastructure, Lamine Mili, Virginia Tech
- GridStat: Middleware for More Extensible and Resilient Status Dissemination for the Electric Power Grid, David Bakken, Washington State University
- Information Embedded Power Systems: Problems and Opportunities for this Critical Infrastructure, Chika Nwankpa, Drexel University
- Sustainable Transport in Europe and Links and Liaisons with America, Roger Stough, George Mason University
- CIP Issues Relevant to Military Avionics, Joseph Cross, Lockheed Martin
- High Confidence Aviation Systems, Brian Williams, MIT
- Safety-Critical Information Technologies for Airborne Systems: Air Transportation and Unmanned Vehicles, Eric Feron, MIT
- Trustworthy Object-Oriented Distributed Embedded Hybrid Systems, Bruce McMillin, °University of Missouri, Rolla
- Technology and Policy in Support of Recovery from Unexpected Events, Yigal Arens, USC/ISI

11:30 — 12:00DISCUSSION AND CONCLUSION OF TECHNICAL MEETING

01:00 — 03:00EU-US ASSESSMENT OF RESEARCH NEEDS: NEXT STEPS (EU co-chair: Andrea Servida, US co-chair: Mark LeBlanc, US co-chair: Stan Riveles)

03:00 — 05:00EU-US GOVERNMENT SESSION (closed session)

Annex 2: List of Participants

S Kamal Abdali
National Science Foundation
kabdali@nsf.gov

Eyal Adar
Itcon-Information Technology
Consultants ltd
eyal@itcon-ltd.com

Frank Anger
National Science Foundation
fanger@nsf.gov

Yigal Arens
USC-Information Sciences Institute
arens@isi.edu

George H. Atkinson
US Department of State
& American Institute of Physics
atkinsongh@state.gov

David Bakken
Washington State University
bakken@eecs.wsu.edu

John S. Bay
DARPA, IEO
jbay@darpa.mil

Henk A.P. Blom
National Aerospace Laboratory NLR
blom@nlr.nl

Sandro Bologna
Ente per le Nuove Tecnologie,
l'Energie e l'Ambiente (ENEA)
bologna@casaccia.enea.it

Raymond Bortner
Air Force Research Laboratory, Air
Vehicles Directorate
raymond.bortner@wpafb.af.mil

Lawrence E. Brandt
National Science Foundation
lbrandt@nsf.gov

Yves Brunet
INP Grenoble
yves.Brunet@inpg.fr

Barrett Bryant
University of Alabama at Birmingham
bryant@cis.uab.edu

Jagdish Chandra
George Washington University
jchandra@seas.gwu.edu

Joseph Cross
Lockheed Martin
joseph.k.cross@lmco.com

Werner Damm
OFFIS, Germany - R&D Division
Safety Critical Systems
werner.damm@OFFIS.de

Francis C. Deckelman
Office of Naval Research
deckelf@onr.navy.mil

Antonio Diu
Red Electrica de Espana
adiu@ree.es

Eric Feron
Massachusetts Institute of Technology
feron@mit.edu

Peter Freeman
National Science Foundation
freeman@cc.gatech.edu

Paul Friessem
Fraunhofer Institut f r Sichere
Telekooperation (FhI-SIT) IBE
paul.friessem@sit.fraunhofer.de

Cita Furlani
National Coordination Office for
Information Technology Research &
Development
furlani@itrd.gov

Helen Gill
National Science Foundation
hgill@nsf.gov

Valerie Gregg
National Science Foundation
vgregg@nsf.gov

Miriam Heller
National Science Foundation
mheller@nsf.gov

Ian Hiskens
University of Wisconsin — Madison
hiskens@engr.wisc.edu

Sally Howe
National Coordination Office for Information Technology Research & Development
howe@itrd.gov

Reinhard W. Hutter
Industrieanlagen-Betriebsgesellschaft mbH (IABG)
hutter@iabg.de

Pradeep K. Khosla
Carnegie Mellon University
pkk@ece.cmu.edu

Steven King
DUST (S&T)
steven.king@osd.mil

Sri Kumar
DARPA
skumar@darpa.mil

Vijay Kumar
University of Pennsylvania
kumar@central.cis.upenn.edu

Carl Landwehr
National Science Foundation
clandweh@nsf.gov

Gwendal Le Grand
ENST
gwendal.legrand@enst.fr

Mark LeBlanc
White House Office of Science and Technology Policy
mleblanc@ostp.eop.gov

Max Lemke
European Commisson
max.lemke@cec.eu.int

David Lounsbury
The Open Group
d.lounsbury@opengroup.org

Ernie Lucier
Federal Aviation Administration
ernest.lucier@faa.gov

Mari Maeda
National Science Foundation (CISE)
mmaeda@nsf.gov

Stephen R. Mahaney
National Science Foundation
smahaney@nsf.gov

Sara Matzner
Applied Research Laboratories at The University of Texas at Austin
matzner@arlut.utexas.edu

Doug Maughan
DARPA
dmaughan@darpa.mil

Roy A. Maxion
Carnegie Mellon University
maxion@cs.cmu.edu

Tom McCutcheon
Dstl, UK
tgmccutcheon@dstl.gov.uk

Philip McKinley
Michigan State University
mckinley@cse.msu.edu

Bruce McMillin
University of Missouri-Rolla
ff@umr.edu

Lamine Mili
Virginia Polytechnic Institute
lmili@vt.edu

James Momoh
National Science Foundation
jmomoh@nsf.gov

Al Mok
University of Texas at Austin
mok@cs.utexas.edu

Priscilla Nelson
National Science Foundation
pnelson@nsf.gov

Norm Neureiter
United States Department of State
Not Available

David Nicol
Dartmouth College & ISTS
nicol@cs.dartmouth.edu

Linda Nozick
Cornell University
lkn3@cornell.edu

Chika Nwankpa
Drexel University
chika@nwankpa.ece.drexel.edu

Rajeev Raje
Indiana University Purdue University
Indianapolis
rraje@cs.iupui.edu

Brian Randell
University of Newcastle upon Tyne
brian.randell@ncl.ac.uk

Ramesh Rao
California Institute for
Telecommunications and Information
Technology
rrao@ucsd.edu

Andrew Rathmell
RAND Europe
rathmell@rand.org

Stanley Riveles
Office of the Science & Technology
Adviser to the Secretary of State
rivelessa@t.state.Gov

Rita V. Rodriguez
National Science Foundation
rrodrigu@nsf.gov

William H. Sanders
University of Illinois at Urbana-
Champaign
whs@crhc.uiuc.edu

Shankar Sastry
University of California Berkeley
sastry@eecs.berkeley.edu

Doug Schmidt
DARPA
dschmidt@darpa.mil

Matthias Schunter
IBM Research
mts@zurich.ibm.com

Ira B. Schwartz
US Naval Research Laboratory
schwartz@nlschaos.nrl.navy.mil

Andrea Servida
European Commisson
andrea.servida@cec.edu.int

Luca Simoncini
Pisa Research Area - CNUCE Institute
luca.simoncini@cnuce.cnr.it

Nozer Singpurwalla
George Washington University
nozer@research.circ.gwu.edu

Jonathan M. Sprinkle
Vanderbilt University
Jonathan.Sprinkle@vanderbilt.edu

John A. Stankovic
University of Virginia
stankovic@cs.virginia.edu

Sue Stendebach
National Science Foundation, CISE
sstendeb@nsf.gov

Roger Stough
George Washington University
rstough@gmu.edu

Gary W. Strong
National Science Foundation
gstrong@nsf.gov

Janos Sztipanovits
Vanderbilt University
janos.sztipanovits@vanderbilt.edu

Simon Szykman
Office of Science and Technology Policy
sszykman@ostp.eop.gov

Lorenzo Valeri
King's College London
lorenzo.valeri@kcl.ac.uk

Sam Varnado
Sandia National Laboratories
sgvarna@sandia.gov

Paulo Jorge Esteves Ver ssimo
Faculdade de Ci ncias da Universidade de Lisboa (FCUL)
pjv@di.fc.ul.pt

Ralph Wachter
Office of Naval Research
wachter@onr.navy.mil

Tim Wallace
Federal Aviation Administration
Timothy.S.Wallace@faa.gov

Carmen Whitson
National Science Foundation
cwhitson@nsf.gov

Brian C. Williams
Massachusetts Institute of Technology
williams@mit.edu

William A. Wulf
National Academy of Engineering
Not Available

ANNEX 3:

CONTEXT AND REPORTS FROM RELATED US AND EU WORKSHOPS

EU Workshop European Requirements for Research and Development in Information Infrastructure Dependability - (19-20 September 2002)

Andrew Rathmell King s College, UK; Reinhard Hutter IABG, D

Dependability Development Support Initiative (DDSI) was an European Commission-sponsored consortium of nine research centers, established to provide policy analysis in support of EU policy on information infrastructure dependability. DDSI ran from June 2001 to November 2002. The project established networks of interested stakeholders in 15 Member States, several associated states and external countries and stimulated an informed policy debate on infrastructure dependability issues.

DDSI's deliverables included a policy summary outlining actions for the EU, Member States and Industry, a conceptual framework, an inventory of national and international activities around the world and focused policy roadmaps in specific areas (public-private partnerships, warning and information sharing and Research & Development).

The R&D vision developed by DDSI identified a clear challenge — societal dependence on unbounded, large scale information infrastructures that constitute socio-technical systems with varying dependability requirements. There is a dependability gap between the capabilities of the technology and social, political and business goals. The goal of a strategic R&D programme must be to close this gap. The research strategy must include a clear research policy, a focus on system of systems level as well as the component level and mechanisms for technology transfer and take-up. The research must integrated findings and methodologies from other disciplines. It must help resolve today's problems and also shape the future Ambient Intelligence environment.

Innovative Information Technologies for Critical Infrastructure Protection - *Shankar Sastry, UC Berkeley, and Janos Sztipanovits, Vanderbilt University*

Long-range research in information technology is crucial to Critical Infrastructure Protection. Today s weak infrastructure is due in large part to the fact that traditional approaches to Digital Control Systems (DCS) and SCADA have not been brought up to the standards of modern information technology. The techniques commonly employed are ad hoc combinations of Proportional Integral Derivative (PID) control and Discrete Event Control. These typically are rudimentary designs focused on control of independent subsystems and provide only limited supervisory and coordination capability. However, today s systems are increasingly coupled and interdependent. The fundamentals of reliable infrastructure have not been adequately worked out for complex networks of highly-interacting subsystems, such as the power grid and the airspace-aircraft environment. These are complex, often dynamically reconfigured, networks. The primary challenge for future generations of these systems is to provide increasingly higher efficiency, while assuring joint physical and logical containment of adverse effects. This is the research agenda of secure network embedded systems.

The NSF/OSTP workshop on September 19th, 20th 2002 began with a number of plenary presentations and contextual discussions of issues in the area of information assurance and survivability, critical infrastructure protection and networking. Two infrastructures, power and air transportation, were highlighted as exemplars to focus on. Several break out sessions were organized to draw out a research agenda to support the most critical needs.

The technology recommendations of our workshop call urgently for new research and development targeted in the following areas (details of the subtasks in the areas are in the report)

- Information Assurance and Survivability
- Secure Network Embedded Systems
- Validated Modeling, Simulation and Visualization of Critical Infrastructure Systems and their Interdependencies

This workshop report develops recommendations on the questions of how to speed up technology transitions of the research into the stakeholder critical infrastructures.

The group felt that it was important that research programs be formulated urgently to begin in FY 2003 by both traditional funding agencies for research: the National Science Foundation, Defense Advance Research Projects Agency, Department of Defense, National Institute for Standards and Technology, and others along with stakeholder agencies like the Department of Energy, the FAA, the Transportation Safety Administration, Department of Commerce, Department of Treasury and other agencies in concert with the establishment of the Department of Homeland Security. The problems are urgent and large. The community is unusually strongly motivated and industry is present at the table to begin a series of very exciting public private partnerships.

Homeland Security Act

Dr. Sam Varnado, Director of Information and Infrastructure Systems, Sandia National Laboratories described the complexity issues, such as cascading effects and interconnectivity, which make it difficult to protect critical infrastructure. Then he described the background and organizational structure of the new Department of Homeland Security.

US efforts to protect the US critical infrastructure were started under the Clinton administration, specifically by Presidential Decision Directive (PDD)- 63 in 1999. This PDD defined the responsibilities for critical infrastructure protection among government agencies, but these responsibilities were not accompanied by funding and little was accomplished.

The tragic 9/11 event changed everything. The Bush Administration reacted quickly to create new government organizations to address the protection of the US homeland. The entire nation recognized the profound challenges to homeland security. The threat is now recognized to be globally pervasive, persistent, ideologically-driven, evolving & learning organization with increasing access to technology, and embedded with noncombatants. Following 9/11, President Bush established the Office of Counter Terrorism to focus on the foreign threat, the Office of Cyber Space Security, and the Office of Homeland Security.

Further, a Critical Infrastructure Protection Board was established to coordinate strategy to protect the homeland. After several months, legislation was introduced to create a new Department of Homeland Security (DHS). HR 5005 passed July 2002. Senate Bill 2452 is under consideration at the time of this writing. The new DHS will have four programmatic undersecretaries - Information Analysis and Infrastructure Protection, Science & Technology, Border and Transportation Security (smart borders), and Emergency Preparedness and Response. It will comprise some 170,000 employees with a budget of around $40B/year. DHS will be formed by transferring responsibilities from a number of other Federal agencies:

Information Analysis and Infrastructure Protection will be formed from NIPC from FBI, National Communications System from DoD, CIAO from DoC, NISAC, and the Federal Computer Incident Response Center.

The Science and Technology Undersecretariat will be formed by transferring the Chemical and Biological Defense Programs from DoE and DoD, the Plum Island Animal Testing Center from the Department of Agriculture and several other programs. It will use the services of the DOE national laboratories for a lot of its needs.

The Border and Transportation Security Undersecretariat will include the US Coast Guard, Customs, Transportation Security Agency and the Bureau of Immigration Enforcement.

The Emergency Preparedness and Response Group will include FEMA, the Nuclear Incident Response groups from DOE and others.

In addition, the Department of Defense has establishment of new entity, North Command. Its role is to provide military support to civilian agencies and to protect the US, Canada, and Mexico during attacks.

In the 9/11 attacks, our infrastructure was used against us. It is almost impossible to predict where the next attack might occur. The US needs to begin thinking of designing its infrastructure to inherently hard, aware and adaptive. It will be impossible to provide 100% protection from all attacks. The concept of self-healing infrastructures may have more merit than trying to protect the entire infrastructure.

US Technical Summary of US Technical Workshop on Information Technology for Critical Infrastructure Protection — Executive Summary

Long-range research in information technology is crucial to Critical Infrastructure Protection. Today s weak infrastructure is due in large part to the fact that traditional approaches to Digital Control Systems (DCS) and SCADA have not been brought up to the standards of modern information technology. The techniques commonly employed are ad hoc combinations of Proportional Integral Derivative (PID) control and Discrete Event Control. These typically are rudimentary designs focused on control of independent subsystems and provide only limited supervisory and coordination capability. However, today s systems are increasingly coupled and interdependent. The fundamentals of reliable infrastructure have not been adequately worked out for complex networks of highly-interacting subsystems, such as the power grid and the airspace-aircraft environment. These are complex, often dynamically reconfigured, networks. The primary challenge for future generations of these systems is to provide everhigher efficiency, while assuring joint physical and logical containment of adverse effects. This is the research agenda of secure network embedded systems.

This NSF/OSTP workshop on September 19th, 20th 2002 began with a number of plenary presentations and contextual discussions of issues in the area of information assurance and survivability, critical infrastructure protection and networking. Two infrastructures, power and air transportation, were highlighted as exemplars to focus on. Several break out sessions were organized to draw out a research agenda to support the most critical needs. An important backdrop to the workshop was the Draft National Strategy to Secure Cyberspace which was released for comment on September 18th, 2000 - the day before the workshop - by the Presidential Critical Infrastructure Protection Board.

The technology recommendations of our workshop call urgently for new research and development targeted in the following areas (details of the subtasks in the areas are in the report)

- *Information Assurance and Survivability*
- *Secure Network Embedded Systems*
- *Validated Modeling, Simulation and Visualization of Critical Infrastructure Systems and their Interdependencies*

This workshop report develops recommendations on the questions of how to speed up technology transitions of the research into the stakeholder critical infrastructures.

This report does not aim to develop specific program recommendations for the inter-agency funding of programs in the three areas listed above. However, the group felt that it was important that research programs be formulated urgently to begin in FY 2003 by both traditional funding agencies for research: the National Science Foundation, Defense Advance Research Projects Agency, Department of Defense, National Institute for Standards and Technology, and others along with stakeholder agencies like the Department of Energy, the FAA, the Transportation Safety

Administration, Department of Commerce, Department of Treasury and other agencies in concert with the establishment of the Department of Homeland Security. The problems are urgent and large. The community is unusually strongly motivated and industry is present at the table to begin a series of very exciting public private partnerships.

information
society
technologies

FET - Future and
Emerging Technologies

DIMACS — Center for
Discrete Mathematics
& Theoretical
Computer Science

European Research Consortium
for Informatics and Mathematics

ERCIM

www.ercim.org

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/