EC Efforts in SCADA-Related Research: Selected Projects

David E. Bakken, Anjan Bose, Carl H. Hauser
School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington, USA
{bakken,bose,hauser}@eecs.wsu.edu

Technical Report EECS-GS-008

20 October 2006

Abstract

This report summarizes selected ICT R&D projects in Europe whose technologies can be used for critical infrastructure protection (CIP), especially the electric power grid. This report also analyzes trends in CIP R&D in Europe. An appendix overviews the EC R&D funding process. This report is the product of a study which the lead author conducted while on professional leave in Europe in the 2004-2005 academic year, as well as followup interactions.

This report was funded by the US National Science Foundation via a supplement to Grant CCR-0326006, funded by both CISE/CNS and OD/OISE, and a travel grant from the Universitetet i Oslo. The views expressed in this document are those of the authors, and not necessarily those of Washington State University, the National Science Foundation or its employees, the European Commission or its employees, or any other entity or person besides the authors.

For updates and additional information, see www.gridstat.net/EC, which the authors intend to maintain for many years. To provide additional information or corrections, please email the lead author.

Table of Contents

1 Introduction

Western societies are increasingly dependent on their electric power and other infrastructures to the extent that their disruption can cause great economic damage and loss of life. Unfortunately, in recent years the construction of long-distance transmission lines has not kept up with the increases in demand for electricity, which has made them more vulnerable to blackouts due to natural disasters or human error. At the same time, the possibility of terrorist disruption of electric power and other critical infrastructures has become a credible and alarming threat.

Governments in the US and Europe have recognized critical infrastructure protection (CIP) as a very important area for both near-term and long-term research and development, given how much their societies depend on critical infrastructures. Electricity is generally considered the most crucial of these infrastructures, given that most other critical infrastructures depend on it. There is widespread recognition that no single country or continent has the ability to solve the many difficult problems related to CIP. As a result, in recent years government research agencies have funded a number of workshops with the explicit goal of helping build international collaboration on CIP research.

The authors of this report have all participated in a number of such workshops, and have been very active in exploring such collaborations with Europe, Japan, and India. They have also been developing a next-generation communications framework, called GridStat, which is designed to give power grids much more flexibility in their communications [GS]. Such flexibility allows a much richer range of control and protection schemes to be utilized in the power grid than is feasible with today's very limited communications infrastructures [GS-PEM,GS-PROCIEEE]. This flexibility in turn helps mitigate the vulnerabilities in the power grid, and allows for more efficient operation (running it closer to physical limits with richer instrumentation and control).

The lead author, Prof. Bakken, spent the 2004-2005 academic year on professional leave in Europe. During this year, he visited a number of colleagues and attended workshops related to the electric power grid, both on the power engineering side and the information and communications technologies (ICT) side.

This report summarizes Prof. Bakken's activities and conclusions related to the electric power grid in Europe that are based on his visits and other transatlantic interactions since. The remainder of this report is organized as follows. Section 2 provides a brief laymen's overview of the electric power grid in Europe. Section 3 summarizes the visits that Prof. Bakken took in Europe, and his observations and conclusions from each visit. It also contains information on followup meetings involving US-EC CIP collaboration planning which the authors attended. Section 4 synthesizes this and other subsequent interactions involving the authors to provide a summary of electric power grid and CIP R&D in Europe. Section 5 concludes. An appendix provides background information on the funding process for the European Commission (EC).

2 Electric Power Grid in Europe

An electric power grid is an enormously complex system. Indeed, the grids in Western Europe and North America are considered the most complex machines ever built. Such grids must simultaneously and in real-time [GS-PROCIEEE]:

- Maintain a very close balance between demand, of which there is little control over, and supply, which the operators of the grid do have some control over;
- Ensure that the generators are all in phase and operating very close to the required frequency (50 Hz in Europe, 60 Hz in North America; renewable units excepted) and voltage (220-240V in Europe, 120 V in North America);
- Deal with the failure of both electricity assets as well as ICT components
- Deal with a wide variety of complex dynamical behaviors whose timescales range from hours down to milliseconds
- Ensure that business requirements (profitable operation) and constraints (avoiding anti-trust situations and interactions) are both met.

The scales of these power grids are enormous; in North America, there are over 3500 companies and other entities whose operational decisions can affect the stability of the grid. Europe has an even larger number with, for example, over 1000 such entities in Switzerland alone.

Grids in developed countries also consist of not only a network of power lines connecting generators and load, but also a communications network overlaid on top of the power infrastructure to help monitor, control, and protect it. This communications network is very limited, which greatly constrains the opportunities for better protection and control [GS-PEM]. This limitation has been widely recognized as a major contributing factor to virtually every recent blackout, including the 2003 blackouts in both Italy and North America.

A map of the main power grid in Western Europe, UCTE, is in Figure 1.

The electric power grids in Western Europe and North America share many similarities beyond the generalizations above. For example, in the control domain, in most of the Western European grid (UCTE grid; not including Scandinavia, the UK, or Ireland) there is frequency control at the EU level as well as secondary control of frequency at the national level; this is identical to the Federal and state/province scheme in North America. There are also wide-area transmission congestion bottlenecks which can make blackouts more likely in both Western Europe (e.g., the Norway-Sweden border) and North America (Pacific Northwest to California, Northeast and Mid-Atlantic to the Midwest, and some parts of the Florida Peninsula). Figure 2 show cross-border power flows on UCTE (courtesy of UCTE).

However, there are differences between the grids in Western Europe and North America. Regulatory issues are generally considered to be more complex in Europe given the larger number of countries involved as well as wider diversity in other areas such as regional economies, and there are more entities whose operational decisions affect the stability of the grid. Also, in Western Europe, there is not only grid-wise voltage control at the top level (as in North America), but also secondary voltage control in France, Belgium, and Italy. Such secondary voltage control is unique worldwide.

The research and development expertise in Europe and the US are similar in most respects, given that the power dynamics are of course the same, and many aspects of their grids are similar. There are some differences in their relative expertise, however. Europe has the world's only experience in secondary voltage control. The US has more experience in the control of deregulated systems, applied where new markets are interacting with old controls. Europe has moved slower and has more carefully engineered such interactions, so it has less experience with them but has found ways to avoid some of the problems that the US has encountered (for example, California's energy bubble a few years ago).

Figure 1: UTCE Western European Power Grid (courtesty of UTCE)

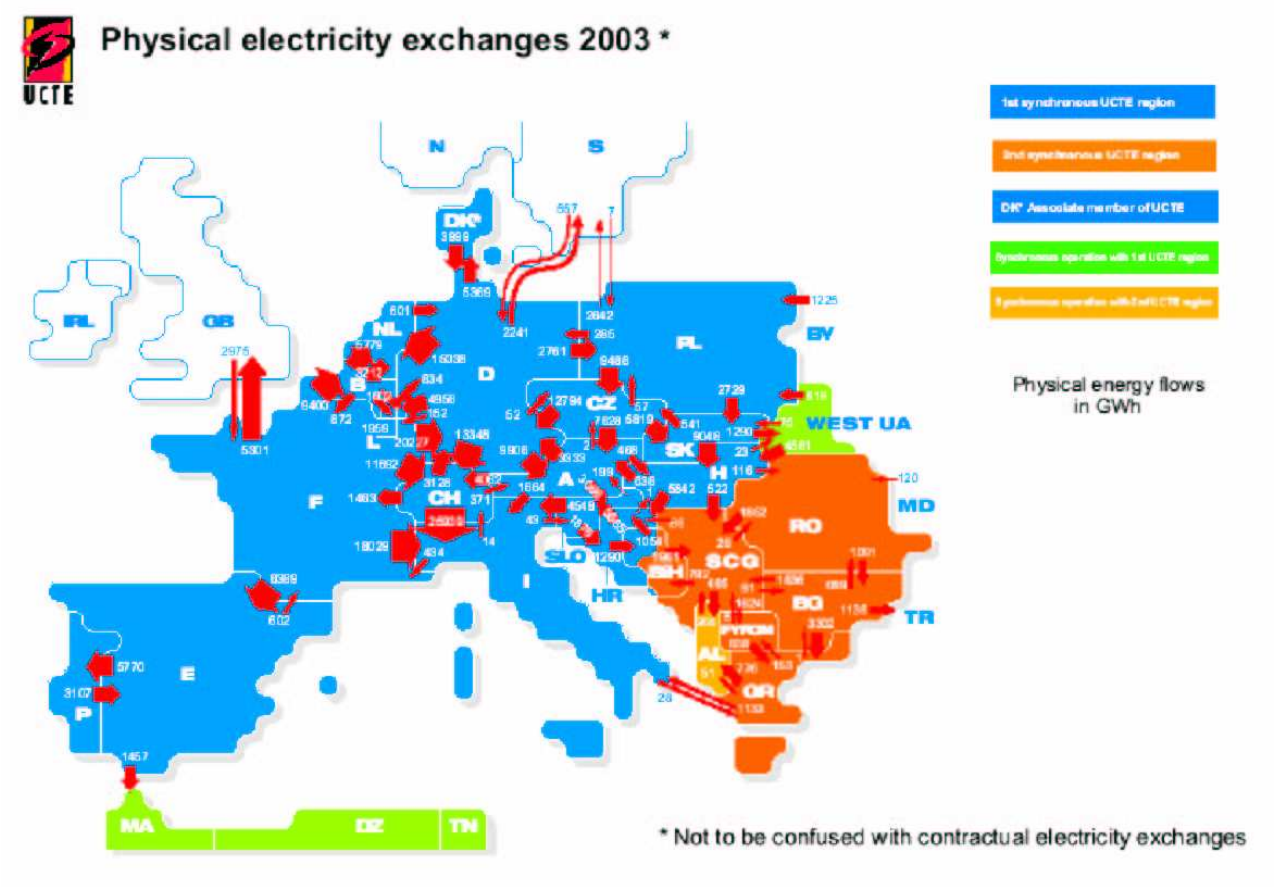

Figure 2: Power flows across UTCE Western Power Grid (courtesy of UTCE)

3 Select Projects & Workshops Related to Electricity & CIP

This section provides an overview of visits which Prof. Bakken made which were partially or completely in support of transatlantic CIP collaboration and the related activity going on at these locations. As such, they offer both a glimpse into CIP-related technical issues under active research in Europe as well as an example of US-EC technical interactions. For more detail than is provided here, please contact Prof. Bakken. The full list of his hosts of these visits is in the Acknowledgements section.

All of the visits below involved technical presentations of GridStat by Prof. Bakken or Prof. Hauser. At many of the university locations and ABB, these presentations lasted 2 hours including vigorous questions and discussion. This was evidence of strong, across-the-board interest in the subject of ICT R&D issues for the electric power grid in particular and more generally ICT for CIP. Finally, in some of the technical areas discussed below, the hosts provided additional followup information on one or more CIP-related projects. These inputs are presented either verbatim or very closely paraphrased.

3.1 European Commission, Belgium

Prof. Bakken visited the European Commission in Brussels on 27 September 2004. He presented a detailed research seminar on GridStat with a long question-and-answer session afterwards. The audience included a number of project managers from both the ICT and power research areas.

Discussions were held with the Unit "ICT for Trust and Security", in the "Network and Communications Technology" branch of the Information Society and Media Directorate-General. A wide range of issues relating to security and the electric power grid were discussed.

Discussions were held with personnel from the Embedded Systems Unit G3 of the Components and Systems Directorate-General. EC Personnel outlined research projects related to CIP in their unit. In particular, a range of transatlantic collaborations which had been considered successful was outlined. As such, these are models for how transatlantic CIP research collaboration has succeeded in the past, and that could be used in the future.

The most lightweight form of such collaboration has been a series of workshops on transatlantic CIP collaboration. These have served to help identify possible research agendas for transatlantic collaboration as well as helping researchers and research agency staff to meet their peers across the Atlantic with whom they could potentially cooperate.

An example of a more concrete form of collaboration which is still relatively *ad hoc* and lightweight involved the NSF. In this effort, 16 EC projects were identified, and NSF sent "dear colleague" letters soliciting interest from its currently-funded researchers. The NSF then picked 4 projects on the US side and funded each for approximately $100K. The EC projects that were involved with this collaboration were:

- DECOS: Dependable Embedded Components and Systems [DECOS]. This project is described further in Section 3.3.1.
- RUNES: Reconfigurable Ubiquitous Networked Embedded Systems [RUNES]. This project is described further in Section 3.7.1.
- ARTIST2: Network of Excellence on Embedded Systems Design [ARTIST2]

- HiPEAC: High Performance Embedded Architectures and Compilers [HiPEAC]

An example of a highly integrated and deep collaboration is the Columbus project [COL04]. This project's research was design of embedded controllers for safety critical systems. The Columbus project involved 2 American universities and 3 in Europe. The funding was balanced with approximately equal funding on each side of the Atlantic.

Finally, discussions were held with personnel from the Enterprise and Industry Directorate-General. EC personnel overviewed the FP process for technology development and how cyber-security research agendas would be formulated for the upcoming FP7. Examples of such formulation activities can be found in an appendix to this document.

Prof. Bakken found great interest in transatlantic collaboration among the EC personnel, something which he uniformly found in subsequent meetings with various EC researchers.

3.2 ABB Research, Switzerland

Prof Bakken visited ABB's Corporate Research Center in Baden, Switzerland [ABB-BADEN] on 6 October 2004. ABB is the largest vendor in the world of components for the electric power grid. This facility is in applied research, much of which supports ABB's power grid products and services in areas of power electronics, electrical insulation, and software application programs.

Prof. Bakken gave a presentation in ABB Research's regular IT Seminar series on GridStat which lasted 2 hours, including a lengthy and vigorous question-and-answer session. The ABB researchers and engineers saw how a much more flexible and managed communications system such as GridStat would be very helpful for ABB's operations. ABB personnel were also interested in US activity involving Phasor Measurement Units (PMUs), such as the DoE's EIPP program with which GridStat is involved [EIPP]. One ABB scientist noted that they spend a lot of money on leased lines for their PMU deployments (which range from the Norway-Sweden border to northern Mexico), which are really only need "a few minutes a year". He was intrigued by the possibility of managed communications with redundant paths and quality of service guarantees supplementing, and perhaps eventually replacing, these expensive lines which are a single point of failure. It was agreed that focused R&D is needed to develop, harden, secure, and validate such ICT, and this could be achievable in a 5-7 year time frame with an ambitious research project.

3.2.1 Project Details: Control and Computation (of Power Dynamics)

One example of a CIP related project follows (provided by ABB):

> **Project Name**: Control and Computation (completed April 2005)
>
> **Project Team**: Verimag, ETH Zurich, CWI Amsterdam, Lund University, Parades GEIE, ABB Switzerland, EdF, University of Siena.
>
> **Funding source**: EC FP6 IST
>
> **Project URL**: http://www.dii.unisi.it/~hybrid/cc/.
>
> **Scope**: New methods for analysis and control design for hybrid systems.

Objectives and Research Issues: The goal of this project was to develop new methods for designing controllers for complex and heterogeneous systems that exhibit both discrete and continuous dynamics. Such systems are called hybrid systems and some of their properties have been studied in recent years by both control and computer scientists. The methodology developed in this project combined classical control techniques (adapted to the hybrid setting) with new reachability-based methods inspired by the verification of discrete systems. In order to maintain a healthy balance between theory and practice, several industrial case-studies were investigated and served as points of reference for the project. From the point of view of CIP, the most important test case was the power system control test cases contributed by ABB. In this test case, blackout avoidance is demonstrated through coordinated applications of switching control actions scheduled by the hybrid control methods proposed by the various other project participants.

Progress: In the Power Systems test case, the hybrid design methods derived in the project have been demonstrated useful as decision logic for a real-time control system such as those we plan as deliverables of a long-term development path at ABB.

CIP/electricity relationship: A follow-up project could involve a hybrid control systems approach to blackout avoidance in electric power systems.

Future plans: We currently do not have any plans on EU funded research in this field. However, we would be open to discussing such possibilities in the context of FP7 or other venues.

The ongoing ABB research has direct and obvious support of CIP, given that it is mainly involved in improving control of the electric power grid.

3.3 Technische Universität Darmstadt, Germany

Prof Bakken visited Technische Universität Darmstadt (Technical University of Darmstadt) in Darmstadt, Germany [TUD] on 8 October 2004.

Lengthy discussions covered a broad range of areas of ICT in which this department is involved which could help harden the electric power grid and other critical infrastructures. These areas fall under the broad area of distributed embedded systems and distributed software, especially the development of robust software, operating systems, and protocols in support of secure and trustworthy systems and services. This research is at the system level for safety critical systems, and involves both algorithmic and architectural issues as well as middleware. Supporting research discussed involved research into real-time event channels and data warehousing.

Much discussion ensued concerning possible transatlantic collaboration involving the hosts' research areas and GridStat. A very active collaboration resulted which eventually involved approx. 15 institutions, including academia (U. Rome, TU Darmstadt, EPFL, and others), key large providers (EDF, ABB Research, Siemens, SAP, and others), and SMEs. However, the proposal did not get submitted given the multitude of bureaucratic details and limited time to resolve them prior to the submission deadline. On the positive side, the active collaboration set up is being sustained and the core researchers involved with this coalition are still actively working together towards a joint, interdisciplinary, transatlantic research project, which they believe may be able to be associated with either the EC's Framework Programme 7 (FP7) [FP7]

or the new NSF CyberTrust center, Trustworthy Cyber Infrastructure for the Power Grid (TCIP) [TCIP] (which the authors of this study are all involved with), or (most likely) both. TCIP involves not only a wide range of focused ICT research for CIP, specifically the electric power grid, but also involves top US electric power researchers.

3.3.1 Project Details: Dependable Embedded Components and Systems

One example of a CIP related project follows (provided by TUD):

> **Project Name**: Integrated Project DECOS (Dependable Embedded Components and Systems)
>
> **Project Team**: ARCS (Gruber), TU Darmstadt (Suri), TU Vienna (Kopetz)
>
> **Funding source**: EC FP6 IST Embedded Systems Unit
>
> **Project URL**: www.decos.at
>
> **Scope**: As the rapidly growing functional and non-functional system requirements (in Dependable/RT Embedded Systems) result in enormous increase in system complexity, it helps to consider component-based design: to provide pre-validated hardware and software components and an appropriate integration methodology for the design of next generation dependable embedded real-time systems. The major objective of DECOS is to perform research in and to develop a set of generic hardware and software components within the framework of the Time-Triggered Architecture. Objectives and Research Issues: DECOS develops the basic enabling technologies to move from a federated distributed architecture to an integrated distributed architecture in order to reduce development, production and maintenance cost and increase the dependability of embedded applications in many application domains. DECOS develops technology invariant software interfaces and encapsulated virtual networks with predictable temporal properties such that application software can be transferred to a new hardware and communication base with minimal effort (legacy re-use).
>
> **Progress**: The DECOS methodology and tools will be evaluated by building three applications in the automotive, aerospace and control domain, respectively. The components and tools developed within DECOS cover: cluster design, middleware and code generators, validation and certification, as well as systems-on-a-chip (SoCs) for high dependability applications.

The research projects outlined in this section (3.3) are highly supportive of CIP. As noted previously, critical infrastructures contain many embedded systems nodes. Providing systematic support for more robust software (with fewer bugs and more tolerant of external failures) as well as providing real-time performance guarantees can readily strengthen most or all critical infrastructures.

3.4 Norsk EnergiRevisjon, Norway

Prof Bakken visited Norsk EnergiRevision [NERAS] in Lier, Norway on 21 October 2004. NERAS is involved with distribution-side management of client's energy, including aggregating realtime loads for better pricing, as well as energy audits of businesses. These technical issues were discussed, and NERAS inquired about the feasibility of opening up offices in the US.

This visit confirmed trends in the US: there is little fundamental research needed solely for the distribution side of the electric power grid which can help improve the control and protection of electric power grids. There is some applied research in the area of "smart loads" which can shed load on a fine granularity when needed, for example the grid-friendly appliances which monitor the grid's operating frequency and shed load when it indicates distress [GRID-APPLIANCE]. However, these and other devices can utilize a next-generation communications infrastructure intended for control and protection on the generation and transmission side, since the requirements for the distribution side are less challenging.

3.5 Linköping University, Sweden

Prof Bakken visited Linköping University in Linköping, Sweden [LINKOP], on 18 November 2004. Discussions were held concerning their real-time research and possible collaborations.

During this visit Prof. Bakken and host Prof. Simin Nadjim-Tehrani started discussions that led to an international workshop (which they played active roles in organizing) the next May entitled "Cyber blackouts: How fast is the recovery, and what preparatory measures do we have in place?"[CIIW05]. This workshop was hosted by the CRIS Instituted and was attended by researchers, practitioners, and government officials from a number of countries and featured invited speakers from the UK, Sweden, US, Italy, and Switzerland.

3.5.1 Project Details: Safeguard and Dependable Distributed Systems

Two examples of CIP related projects follows (provided by Linköping):

> Simin Nadjim-Tehrani at Dept of Computer and Information Systems at Linköping university (LiU) has been recently involved in two European projects that focus on the role of software in critical networks. The first project, Safeguard, was a project running 2001-2004. In this project vulnerabilities and threats to large critical infrastructures were studied, and techniques to safeguard such networks were tested in communication and control layers of electricity networks (SCADA systems), as well as operation and management layers of telecom networks.
>
> The project was granted pre 9/11, so it was a pioneering project in this area in Europe. The results of the projects have been published in numerous publications including a book chapter in a recent book on dependability [SAFE-CIP]. A major result of the project, developed at LiU has been an adaptable real-time anomaly detection algorithm that has been tested with good results on IP packets generated in a test network at the Swiss main telecom operator Swisscom. This spring the group is planning to test the same algorithm on detecting anomalies in water supply systems, in cooperation with the University of Cincinnati. The algorithms developed in the project were implemented as safeguard agents built on top of an efficient and flexible agent platform.
>
> A running project in the area of dependability in which the same PI is active is called DeDiSys (Dependable Distributed Systems). The project goal is to extend existing component-based middleware in order to deal with on-line trade-offs between availability and consistency of data. The main application area of the project is air traffic control, and the distributed object system will be shown to exhibit higher availability during periods of network partition, when the existing (not partition-tolerant) middleware would be

simply unable to deal with the fault and stop servicing requests. This project runs 2004-2007, and has already resulted in a few publications.

The projects outlined above are very supportive of CIP. Systematic support for safety-critical applications (one which must avoid a catastrophic failure) has obvious applicability. Component-based software engineering is widely recognized as part of best practices in software engineering, so providing systematic support for enhancing availability, and trading it off with consistency so as to provide appropriate performance for a given application or service, can be very helpful to CIP. Similarly, the workshop which was initiated during the lead author's visit explored how well the state of the practice in ICT supports critical infrastructures, namely ICT service outages and what can be done about them.

3.6 EC Workshop on power grid communications, Belgium

Prof Bakken attended an EC workshop "The Future of ICT for Power Systems: Emerging Security Challenges" in Brussels, Belgium February 3–4, 2005 [RAMI05]. He presented one of the keynote talks, "Next-Generation Grid Communication Requirements and Research Issues". Note: in this workshop discussion, please be aware that the term "security" is used in the power grid sense, i.e., reliability or stability; it does not mean cybersecurity.

This workshop aimed to promote discussion among the industry and researchers on the role of pervasive information & communication technologies (ICT) in the European electric power grid, and help identify and discuss key R&D challenges in this area that could be addressed by the upcoming Framework Programme 7 (FP7) [FP7]. The workshop was jointly organized by the Directorate Generals for Information Society and Media, Research, and Joint Research Centre. The workshop was attended by approx. 60 people, with a roughly even split between industry and academia and approx 10 EC personnel.

The workshop aimed to achieve consensus in the following areas [RAMI05-REPORT]:

1. methods to assess power system vulnerabilities, risks and potential impact of blackouts;
2. methods to improve power system controls and protections in light of security risks;
3. advanced system controls and communications technologies to improve prevention, protection and defence including SCADA, wide area measurement, etc considering also the necessary collaboration with the foreign supply countries
4. vulnerabilities associated to increased control complexity and openness of the supporting information and communication technologies.

The first area concerned risk assessment. Participants discussed the challenges involving adequate techniques to forecast and assess the impact of blackouts, the overall reliability of the European power grid, and the lack of experienced operators. Technical issues discussed include new techniques for assessing a chain of events which can lead to a blackout and more integrated and faster state estimators being placed in the control loop. Policy issues which were discussed include the low level of investment by the power sector in equipment and R&D, who should pay for this extra security and how much it will cost.

The second area concerned methods to improve control of the electric power grid in Europe. Participants discussed how liberalization was creating more threats and vulnerabilities, how to deal with a trend towards distributed generation (including renewable energy), and the trend

towards using more off-the-shelf systems. Technical issues discussed involved the tradeoffs inherent in using formal methods, integration of fast/responsive security into complex control and monitoring systems, a trend towards more intelligent distributed control, and the integration of heterogeneous modeling methods into power grid operations. Policy issues discussed included dealing with legacy systems, humans in the loop, and costs of power grid security.

The third area concerned advanced systems controls. Participants discussed emerging cyber threats of SCADA systems, advanced control and communications technologies, and the resilience of the telecom infrastructure which in part underlies SCADA. Technical issues discussed included migration paths of new technologies which are non-intrusive and smart local protection and control. Policy issues discussed included the cross-border weaknesses of EU grid controls, the overcoming the problem of economically-biased control, and the need to deal with cyber-vulernabilities.

The fourth and final are concerned these cyber vulnerabilities. Participants discussed technological trends which are greatly increasing vulnerabilities, including the narrowing of boundaries between the business and control sides of electric power in Europe, a move towards wireless network protocols, stronger integration of control and communications, and attacks on power grid protocols. Technical issues discussed concerned identification and modeling of such threats, how to use risk assessment and security criteria in order to plan and operate communications networks for the power grid, and how to make security be a more systemic property rather than an afterthought. Policy issues involved the risks associated with the spread of monoculture and the role of standardization in this area.

The report on this workshop can be found at [RAMI05-REPORT]. This workshop directly supports the goals of CIP in helping to organize EC CIP research that will happen during FP7, both in helping define consensus for particular research issues for ICT and the power grid, as well as helping form a research community and emerging project partnerships among its attendees.

3.7 Lancaster University, UK

Prof Bakken visited Lancaster University in Lancaster, UK on April 22 and 25 [LANC].

Lancaster professors and students presented overviews of their research on middleware, including mobility support, component-based services, dynamic reconfiguration, and self-managing applications and services built using next-generation middleware.

There was much discussion on possible collaborations. In particular, the use of reflective models for a wide-area deployment of GridStat seemed a promising approach that could help organize and manage a complex infrastructure in a way which would enable automatic adaptations in this communications infrastructure. Discovering and programming candidate adaptations would be very time consuming without such systematic assistance, so such automatic adaptations could help enable some facets of CIP to be feasible much sooner than would otherwise be possible.

3.7.1 Project Details: Reconfigurable Ubiquitous Networked Embedded Systems

One example of a CIP related project follows (provided by Lancaster):

Project Name: Runes: Reconfigurable Ubiquitous Networked Embedded Systems

Project Team: 22 partners from 8 countries: Australia, Germany, Greece, Italy, Hungary, Sweden, UK, and the US. For the detailed list of partners see the project URL below.

Funding source: EC FP6

Project URL: http://www.ist-runes.org/

Scope: We stand on the brink of a revolution, in which the worlds of the embedded system and the Internet will collide. This will lead to the construction of the first truly pervasive networked computer systems and thus open up a marketplace of a scale unparalleled in the history of technology. To realise this commercial potential requires a research and development programme focused on the creation of the infrastructure that actively promotes the efficient and inexpensive construction and management of novel services and applications that are predictable and intuitively usable, so as to fulfill the global user expectations for invisible computing.

The RUNES project represents the first major European effort in this area. Much current embedded systems development is bespoke. However, the environments we envisage are more complex than today's limited, controlled, deployments. This complexity is a consequence of heterogeneity, dynamicity, and scale, which means that bespoke development is too expensive and too limiting for innovative applications. To control complexity, we believe that it is necessary to build scaleable middleware systems and application development tools that allow users, designers, and programmers the flexibility to interact with the detailed environment where necessary, whilst affording the clarity that allows for ease of application construction and use.

Objectives and Research Issues: The specific objectives of RUNES are as follows:

- to build middleware systems that are adaptive and intelligently self-organising
- to ensure middleware is robust and predictable enough to make computing truly invisible
- to build tools that allow for the automated assessment of usability, and that allow applications to be debugged
- to assess our developments in both real-world scenarios and emulations of large scale systems

Progress: In terms of the middleware, strong progress has been made on the overall architecture, the underlying lightweight component model that supports configurability and also on implementations of an associated component run-time for a variety of environments in a variety of languages (e.g. Java and C).

CIP/electricity relationship: The Runes middleware is both lightweight and configurable for a variety of networked systems. It can also support a variety of interaction types including for example publish-subscribe. This work can therefore support a more abstract programming environment as required for this area but also one that can be tailored for the unique characteristics of power grids.

Future plans: Application of the middleware to a variety of networked embedded environments including for example power grids.

The Computing Department at Lancaster [LANCS-CS] is widely recognized as one of the finest ones in Europe. It is also arguably the top department in the world in terms of middleware research. Middleware is a very crucial supporting technology for future CIP deployments because it provides interoperability across heterogeneous environments (operating system, network technology, CPU type, programming language) and provides programmers with higher-level building blocks. In particular, this department has many projects ongoing that are related to reflective middleware [LANCS-REFL]. In a reflective system it is possible to reason about the internal structure of a system and make adaptations based on this self-knowledge. This capability has direct applicability to CIP, because the scale of such systems requires highly automated reconfiguration and other adaptations. Reflection shows great potential to be a fundamental building block to support such adaptability.

3.8 Workshop on Next-Gen. Power Grid Communications,Italy

Prof Bakken attended an informal workshop, "Next-Generation Communication Infrastructures for Better Control and Protection of the Power Grid", and gave the keynote address, "Future Power Grid Communications in the US: GridStat and EIPP". Prof. Bakken helped organize this workshop along with its host, Prof. Roberto Baldoni of Università degli Studi di Roma (University of Rome)[UROME].

This workshop was attended by approx 25 participants, mostly from the electric power industry in Italy. The workshop featured discussions of ICT research which can help protection and control of the power grid, as well as a number of experiences and case studies involving various interactions between the power dynamics and the ICT of Italy's electric power grid.

3.9 Simula Research Lab, Norway

Prof. Bakken visited Simula Research Lab [SIMULA] 20% FTE during his sabbatical. Simula has wide experience in applied distributed computing research, among other areas. Much discussion was held involving the use of QoS-aware component technologies, mobile middeware, and adaptive middleware.

3.9.1 Project Details: Mobility and Adaptation-Enabling Middleware

One example of a CIP related project follows (provided by Simula):

> **Project Name**: Mobility and adaptation-enabling middleware (MADAM)
>
> **Project Team**: 8 partners from Norway (3), Germany (2), Italy (1), Spain (1), and Cyprus (1).
>
> **Funding source**: EC IST
>
> **Project URL**: www.ist-madam.org
>
> **Scope**: Computers and networking technology are becoming an integral part of our living and working environment. The increasing mobility and pervasiveness of computing and communication enables new services and applications that can improve quality of work and life. However the constant change that characterizes mobile environment – e.g. network, battery, light and noise conditions – pose a significant challenge to developers. To retain usability, usefulness, and reliability applications need

to adapt to the changing operating environment and the context in which they are used. The MADAM middleware will support such dynamically adaptive applications.

Objectives and Research Issues: To achieve this objective we will study the adaptivity requirements of mobile applications and develop a theory of adaptation. A set of reusable adaptation strategies and adaptation mechanisms, based on a dynamically reconfigurable component architecture will be developed. Modelling language extensions and tools will enable application designers to specify adaptation capabilities at design time.

Progress: An overall architecture has been specified and a first prototype has been realized. Two commercial applications have been ported and refactored to run on the MADAM middleware. This includes externalizing the adaptation logic from the application code. First evaluation results (qualitative, quantitative) are soon to be published.

CIP/electricity relationship: Relevance of MADAM is the support for context-aware adaptation planning (planning-based middleware) and the tool support for developing context-ware adaptive applications and services. MADAM supports adaptation to both foreseen and unforeseen context changes: Its adaptation policies are goal-oriented only dependent on the extra functional properties of a service. This is in contrast to action (rule-based) policies that require the policy designer has deep knowledge of the implementation of a service.

Future plans: In future projects we will address adaptation mechanisms complementing architectural adaptation such as aspect weaving, support for dependable adaptation, decentralized adaptation planning, support for planning of service architectures such as service overlays and peer-to-peer (MADAM is limited to client-server), planning support for dynamic service discovery, and the use of MDD for building self-adaptive applications in an industrial context.

The research projects outlined in this section (3.9) are supportive of CIP. Having reusable adaptation strategies which are well-understood could enable programmers to much more readily program critical infrastructures. Support for mobile devices is also important, because these devices are playing an increasing role in critical infrastructures, for example an electric company repairman accessing a substation to help restart an electric grid after a blackout or simply a substation with wireless LAN connectivity (which is becoming attractive for utilities to consider for economic reasons).

3.10 US-EU Workshop on Large ICT-based Infrastructures and Interdependencies

Profs. Bakken and Hauser attended a Joint US-EU Workshop "Large ICT-based Infrastructures and Interdependencies: Control, Safety, Security and Dependability" on March 16-17 in Washington, DC [US-EUMarch06a]. The main goals of this workshop were [US-EUMarch06b]:

1. To foster technical collaboration between the US and the EU on increasingly ICT-centric infrastructures;
2. Joint roadmapping of research activities between the US and EU on areas of common importance in the area of ICT enabled critical infrastructures and interdependencies;

3. To identify strategic opportunities for cooperation in preparation for new research programs, such as Framework Program 7 for the EC and program directions for FY 2007 and forward by the NSF and other US agencies.

Researchers from industry and the academe in both the US and Europe presented research challenges and project summaries; European countries represented included Italy, UK, Sweden, Germany, Austria, and Portugal. Government officials from the US and EC were also present and summarized opportunities and potential future collaborative directions. Many of the workshop participants commented to the authors or to the group that they learned of many valuable collaboration opportunities on specific technologies under development on the other side of the Atlantic.

3.11 International Workshop on Complex Network and Infrastructure Protection

Prof. Hauser attended the *International Workshop on Complex Network and Infrastructure Protection*, hosted by the Italian National Agency for New Technologies, Energy, and the Environment (ENEA) and The International Emergency Management Society (TIEMS), and presented a research paper. This workshop was held March 28-29 in Rome, Italy. Its goal was [CNIP06] to

> bring together experts, infrastructures specialists and stakeholders, with different cultural and scientific backgrounds, to address and analyse the following aspects of Complex Networks and Infrastructure Protection:
>
> - Proposing methods and tools to analyse and understand new risks and vulnerability.
> - Giving practical solutions to reduce and mitigate potential dangerous effects.
> - Identifying strategies and tools to support emergency managers during critical events.

Many researchers and funding agencies consider this goal important given the interdependence of critical infrastructures in the US and Europe. Papers were presented by authors from Italy, the US, Belgium, Croatia, Spain, Canada, Australia, UK, Sweden, and other countries. Research issues discussed included trust, security, dependability, and interdependence in many domains, including the electric power grid, telecommunications, and emergency response.

3.12 ENEA Workshop on Complex Networks and Infrastructure Protection

Prof. Bakken attended the *Workshop on Complex Networks and Infrastructure Protection*, hosted by the Italian National Energy Lab (ENEA) in Rome, Italy, on June 6, 2006 [ENEA06]. Technical issues involving CIP were discussed, including security and trust in the electric power grid, dependable systems software, methods and tools supporting CIP, and vulnerabilities of human organizations. The organizers remarked that one of their biggest successes in the last 5 years has been getting interdisciplinary R&D to support CIP identified as a key future topics for applied R&D, which is very consistent with the authors' observations as reported elsewhere in this report.

3.13 Summary Comments

There is a wide spectrum of research underway in Europe supporting CIP, in fact there seems to be much more research involving large teams of researchers, something which is crucial in helping develop an integrated set of technologies (as opposed to point solutions) urgently needed by CIP. Such large-team ICT research is rarely funded in the US today.

There appears to be great interest with both the EC and researchers to broaden this CIP research in FP7 to be even more interdisciplinary and to begin to deploy it directly in critical infrastructures, especially the electric power grid. The broad area of CIP thus seems well-suited for mutually-beneficial transatlantic research.

Things seem to be lining up reasonably well here for collaborations involving FP7. The main calls for proposals related to the topics addressed in this section will come out in Fall, 2007. While there is nothing in the current government fiscal year (GFY07) which started October 1, 2006, GFY08 lines up well. A recent article by an NSF official mentioned the importance of international activities in ICT [Fre06] and thus gives hope that GFY08 may include concrete support on the US side for CIP-related collaborations.

4 Trends in Electric Power Grid and ICT-CIP R&D in Europe

This section overviews trends which the authors have observed in Prof. Bakken's year in Europe as well as with numerous workshops and technical discussions since. It is by no means a comprehensive list of such trends.

4.1 R&D Trends for Electric Power

The R&D trends for electric power are in many regards quite similar to those of the US, due to the similarities of their power grids and of enabling technologies that are becoming available. The main areas for new or increased electricity research in Europe are distributed generation, renewable energy, and smart energy networks. These areas do have some overlap, and as a whole they involve a restructuring of how entities in the power grid interact, react, and are controlled [WMB05]. Enabling this is a systematic application of ICT technologies, the roadmap has been being developed for Europe in the last few years, and is expected to accelerate in FP7.

Distributed generation (DG) R&D is helping move electric grids from centralized, large-scale power plants (usually using fossil fuels) that transmit much of the power over large distances towards an architecture where much more power is generated by distributed energy resources (DER) that are much closer to the customers [DGEN-INTRO]. DG projects from FP5 (and the lessons learned) can be found in [FP5-SMART], which also is a very good layman's overview to many electricity related issues. DG projects underway in FP6 can be found in [DER-FP6].

Renewable energy (RE) includes wind, solar, and tidal sources and is a major and growing emphasis in Europe in recent years, both for environmental reasons as well as achieving the benefits of DG. Unlike conventional generators based on fossil fuels or hydro, generators from some kinds of renewable sources such as wind do not operate in a frequency synchronized with other generators. Part of the smart energy networks vision in Europe includes achieving a better understanding of how such non-synchronized generators impact the stability of the grid, and how any negative affects can be mitigated.

Smart energy networks is a broad, overarching area which encompasses not only DG and RE but also other topics such as how to better control the grid with better communications and more controllable devices and generators. Indeed, a recent EC report outlines preliminary research areas likely to be included in FP7 in order to help achieve this vision [FP5-SMART]. The first area listed is as follows:

> **Intelligent electricity networks**. RTD should cover the development of new concepts, system architectures and a regulatory framework for control, supervision and operation of electricity networks, so as to transform the grid into an interactive (customers/operators) service network, while maximizing reliability, power quality, efficiency and security. These systems should be based on applications of distributed intelligent, plug and play, e-trading, power-line communications, etc.

The details of how this part of the FP7 smart energy vision will be realized in FP7 priorities are under active development [PLAT06]. The trends in ICT research in Europe supporting this goal of intelligent electricity networks are overviewed in Section 4.2.

Finally, many European (and American) researchers and practitioners in electricity seem to believe that **phasor measurement units** (PMUs) have great potential to help enable better control of the power grid. This key enabling technology allows the control of power grids to move away from the traditional techniques of state estimation, which is computationally expensive and slow, towards state measurement, which is both more accurate and faster. Utilizing PMUs for controlling the grid requires sending the PMU data to remote sites with reliable, fast, and secure computer networks.

There are research trends in other electricity-related areas such as power dynamics, control theory, energy storage, fuel cells, and superconductivity which are not included in this analysis of trends. Such areas are outside the scope of this document; they are outside of the lead author's expertise and interactions with Europe, mainly because they are not nearly as closely related to ICT as are the topics analyzed in this section.

4.2 R&D Trends in ICT for CIP

There has been a widespread realization in Europe of the need for CIP and the key role that ICT R&D plays in this. An example of a current workshop on this topic is [CNIP06], as overviewed in Section 3.11, and this recognition is prevalent in many EC reports and programs

Critical infrastructures in Europe (and the US) have historically been built from a "system" perspective. For example, the state of the art is capable of building critical infrastructures which are

- *Application-specific*: designed only to accommodate a fixed and known set of application programs (generally only the ones that were designed when the infrastructure was built)
- *Domain-specific*: designed only for the needs of the domain of the particular infrastructure
- *Technology-specific*: designed to utilize only the technologies available when the infrastructure was created, and often only a subset of them.
- *Topology-specific*: designed to support a particular, fixed communications topology between entities in the infrastructure.
- *QoS-specific*: designed only to support a quality of service (QoS) and security which is specified when the system is created, and can not easily provide other tradeoffs.

There is widespread recognition in Europe (and the US) in recent years that the state of the art results in critical infrastructures that are far too expensive and brittle, and does not provide adequate CIP. Research in Europe in the next decade is likely to try to extend the state of the art to remove some or all of the limitations outlined above. For example, removing application-specific limitation would allow an infrastructure to much better support more application programs as current ones evolve and new ones are devised. Removing domain-specific limitations would allow CIP R&D to be leveraged much more effectively across multiple critical infrastructures. Removing technology-specific limitations would allow critical infrastructures to much more easily "ride the technology curve" and incorporate new networking and other QoS and cyber-security related technologies as they become available. This helps the infrastructure to improve as it evolves much more easily. Removing topology-specific limitations would help critical infrastructures much more readily be extended to accommodate new infrastructure assets

and long-term changes in patterns of communication between them. Removing QoS-specific limitations would help provide a wider set of QoS and security properties, and tradeoffs between them, for current and future applications for a given critical infrastructure.

Current research, and especially that which seems likely to be initiated as part of FP7, aims to remove as many of the above limitations as far as is possible. Two general areas that aim to facilitate this are called in Europe (and elsewhere) *pervasive computing* with *ambient intelligence* and also *service-oriented architectures*. Pervasive computing aims to remove many or all of the above limitations and help infrastructures to be more resilient and responsive while supporting a much wider scale of devices. Ambient intelligence research in part helps deal in a systematic manner with the trend that there is much more intelligence and overall capabilities at the edges of critical infrastructures. Issues here in general involve helping this trend be a strong positive which can add to the resilience of the infrastructure rather than the liability it can be if not properly integrated and controlled. Service-oriented architectures (SOA) are an effort in distributed computing and software engineering to help provide techniques to let infrastructures be built more with a service-oriented approach (which can help remove the above-mentioned limitations) rather than the limited system-oriented approach of today.

The above trends can be observed in a number of EC workshops and other technical conferences in Europe, but [RAMI04], [ISAS05], and [CNIP06] are good starting points.

4.3 Summary Comments

There is a widespread recognition in both Europe and the US among electricity R&D personnel in academia, research, and government that there needs to be a systematic and well-planned integration of ICT into the electric power grid. These ICT-based services are seen as a key enabling technology for smart energy and distributed generation. It is understood that such ICT-based services are more than just "plugging in a network" [GS-PEM]. However, there is a deeper understanding among the electricity community in Europe, and more generally in its CIP community, that the development of such ICT-based services requires a systematic, applied research program to develop such comprehensive services with an appropriate degree of cyber-security, performance, resilience, scalability, and flexibility. There is a recognition on both sides of the Atlantic that part of this work involves the need for a much better understanding how the dynamics of the power grid's communications network (whether today's limited one or the next generation thereof) affect the grid's power dynamics. However, Europe seems more likely to launch interdisciplinary research in this area in the near future, via FP7.

5 Conclusions

Electric power grids in Europe and the US, as well as other critical infrastructures, face largely the same set of problems with respect to hardening and protecting them. Operation of electric grids in particular must deal with complicated electrical phenomena over wide geographic areas with communications technologies which are widely recognized as inadequate. At the same time, there is widespread recognition in Europe and the US and elsewhere that no single country or even continent can solve CIP issues in a reasonable amount of time. Major blackouts in both Europe and the US in 2003 have added particular urgency on both sides of the Atlantic to harden the electric power grid in particular.

This report summarizes activity and analyzes R&D trends in Europe related to ICT and the electric power grid. Research in Europe, emerging in both electric power control and ICT, holds promise in making progress in CIP.

The authors believe that there are many possible collaborations involving CIP which are mutually beneficial to both Europe and the US. Indeed, in electric power R&D, Europe is stronger in secondary voltage control while the US is more experienced with control in deregulated environments. In ICT R&D, Europe is stronger in embedded computing and dependable computing, while the US is stronger in cyber-security. The authors believe there is much mutual benefit from some focused programs for transatlantic collaboration and cooperation. This has been recognized for at least 4-5 years in Europe (see for example [SEC-PREP-PERSON, FP5-SMART]), and momentum seems to have grown significantly in the last few years in the US.

Acknowledgements

The authors thank the US National Science Foundation for making this survey possible via a supplement to Grant CCR-0326006, funded by both CISE/CNS and OD/OISE. The authors also thank the Universitetet i Oslo for a travel grant which helped with some of these trips.

The lead author thanks the hosts during his visits of CIP-related projects in Europe: Technische Universität Darmstadt: Prof. Neeraj Suri and Prof. Alexandro Buchmann,; ABB Research: Dr. Mats Larsson, Dr. Otto Preiss, Dr. Tatjana Kostic, Dr. Claus Vetter; Technische Universität Wien: Prof. Hermann Kopetz; Linköping University: Prof. Simin Nadjim-Tehrani and Prof. Jörgen Hansson; Lancaster University: Prof. Gordon Blair and Prof. Geoff Coulson; Università di Roma "La Sapienza": Prof. Roberto Baldoni; Simula Research Lab: Prof. Frank Eliassen; Universitetet i Oslo: Prof. Thomas Plagemann; Norsk EnergiRevision: Mr. Thomas Hakavik.

The lead author is also thankful for many fruitful technical and programmatic discussions with European Commission staff, including Mr. Andrea Servida, Mr. Alkis Konstantellos, Ms. Christiane Bernard, Mr. Stefano Puppin, Mr. Alberto Stefanini, Mr. Jacques Bus, Mr. Marcelo Masera, and Dr. Angelo Marino.

Special thanks go to Prof. Neeraj Suri for his many helpful discussions on EC programmatics as well as CIP-related issues in dependable computing and embedded computing; to Andrea Servida for his many encouragements and discussions; to Prof. Rachid Guerraoui of Ecole Polytechnique Fédérale de Lausanne (EPFL) and Prof. Christof Fetzer of Technische Universität Dresden and Dr. Aad van Moorsel of the University of Newcastle Upon Tyne for their discussions about CIP-related issues; to Dr. Mats Larsson of ABB and Dr. Sandro Bologna of Ente per le Nuove tecnologie, l'Energia e l'Ambiente (ENEA) for the discussions about the intersection of power dynamics and ICT; and to Prof. Bill Sanders of University of Illinois for discussions regarding TCIP and European CIP research. Finally, many thanks go to Beth Bakken and Ginny Hauser for proofreading this document.

The authors apologize in advance for any omissions in the above.

The views expressed in this document are those of the authors, and not necessarily those of Washington State University, the National Science Foundation or its employees, the European Commission or its employees, or any other entity or person besides the authors.

References

[ABB-BADEN] research.abb.ch

[ARTIST2] www.artist-embedded.org/FP6/

[CNIP06] International Workshop on Complex Network and Infrastructure Protection, ENEA/IEMS, March 28-29, Rome, Italy, http://ciip.casaccia.enea.it/cnip06/

[CI2RCO] http://www.ci2rco.org/

[CIIW05] The first CRIS International Workshop on Critical Information Infrastructures (CIIW'05)—"Cyber blackouts: How fast is the recovery, and what preparatory measures do we have in place?", CRIS Institite (www.cris-inst.com), May 17-17, 2005, Linköping, Sweden. http://www.ida.liu.se/conferences/CIIW05/.

[CNIP06] *International Workshop on Complex Network and Infrastructure Protection*, ENEA and TIEMS, March 28-29, Rome, Italy, http://ciip.casaccia.enea.it/cnip06/

[COL04] COLUMBUS project final report home page, http://www.columbus.gr/finalreport/welcome.htm

[DECOS] www.decos.at

[DER-FP6] European Commission, European Distributed Energy Resouces Projects, EUR 21239, ISBN 92-894-800-7, http://www.iss-eu.org/activ/content/gop.pdf

[DGEN-INTRO] EC, Introduction to Distributed Generation, http://europa.eu.int/comm/research/energy/nn/nn_rt/nn_rt_dg/article_1158_en.htm

[EIPP] http://phasors.pnl.gov/

[ENEA06] Workshop on Complex Networks and Infrastructure Protection, Italian National Energy Lab (ENEA), Rome, Italy, 05 June 2006, http://www.cresco.enea.it/SPIII/SPIII2/evento-june06/program5-06.htm

[FP5-SMART] European Commission, Towards Smart Power Networks: Lessons Learned from European Research FP5 Projects, 2005, ISBN 92-79-00554-5, EC document EUR 21970, http://europa.eu.int/comm/research/energy/pdf/towards_smartpower_en.pdf.

[FP7] http://www.cordis.lu/fp7/home.html

[Fre06] Freeman, Peter. "Another Year, More Dollars", *Computing Research News*, 18(4), Computing Research Association, September 2006, http://www.cra.org/CRN/articles/sept06/freeman.html

[GRID-APPLIANCE] http://gridwise.pnl.gov/technologies/transactive_controls.stm

[GS] www.gridstat.net

[GS-PEM] Carl Hauser, David Bakken, and Anjan Bose. "A Failure to Communicate: Next-Generation Communication Requirements, Technologies, and Architecture for the Electric Power Grid", *IEEE Power and Energy*, 3(2), March/April, 2005, 47–55. Available for fair-use, research purposes only at http://gridstat.net/intro.pdf.

[GS-PROCIEEE] Kevin Tomsovic, David Bakken, Mani Venkatasubramanian, and Anjan Bose. "Designing the Next Generation of Real-Time Control, Communication and Computations for Large Power Systems", *Proceedings of the IEEE (Special Issue on Energy Infrastructure Systems)*, 93(5), May, 2005. Available for fair-use, research purposes only at http://gridstat.net/Power-GridStat-ProceedingsIEEE.pdf.

[HiPEAC] www.hipeac.net

[ISAS05] http://www.informatik.hu-berlin.de/rok/isas2005.html

[LANC] www.lancs.ac.uk

[LANCS-CS] http://www.comp.lancs.ac.uk/

[LANCS-REFL] http://www.comp.lancs.ac.uk/computing/research/mpg/reflection/projects.php

[LINKOP] http://www.ida.liu.se/

[NERAS] www.neras.no

[PLAT06] EC, Technology Platform for the Electricity Networks of the Future, http://europa.eu.int/comm/research/energy/nn/nn_rt/nn_rt_dg/article_2262_en.htm

[RAMI04] "Resilience in Ambient Intelligence (RAmI): Report of the Workshop Held in Brussels, 19 March 2004", https://rami.jrc.it/workshop/W_Report.pdf

[RAMI05] Workshop "The Future of ICT for Power Systems: Emerging Security Challenges", https://rami.jrc.it/workshop_05/ . Note here that "Security" is in the power context, i.e., meaning approximately what ICT personnel call stability and reliability.

[RAMI05-REPORT] https://rami.jrc.it/workshop_05/Report-ICT-for-Power-Systems.pdf

[RUNES] www.ist-runes.org

[SAFE-CIP] D. Gamez, S. Nadjim-Tehrani, J. Bigham, C. Balducelli, T. Chyssler, and K. Burbeck, Safeguarding Critical Infrastructures, Chapter 18 in Dependable Computing Systems: Paradigms, Performance Issues and Applications, John Wiley & Sons, 2005.

[SEC-PREP-OVER] ftp://ftp.cordis.lu/pub/era/docs/communication_security_030204_en.pdf

[SEC-PREP-PERSON] Research for a Secure Europe: Report of the Group of Personalities in the Field of Security Research, European Commission, ISBN 92-894-6611-1, http://europa.eu.int/comm/enterprise/security/doc/gop_en.pdf.

[SEC-PREP-PROJ1] http://europa.eu.int/comm/enterprise/security/articles/article_2164_en.htm

[SEC-PREP-PROJ2] http://europa.eu.int/rapid/pressReleasesAction.do?reference=MEMO/05/277&format=HTML&aged=0&language=EN&guiLanguage=fr

[SEC-HOME] http://europa.eu.int/comm/enterprise/security/index_en.htm

[SIMULA] www.simula.no

[TCIP] TCIP: Trustworthy Cyber Infrastructure for the Power Grid, NSF CyberTrust Center, http://tcip.iti.uiuc.edu/tcip/ 2005,

[TUD] www.informatik.tu-darmstadt.de

[TUW] http://www.tuwien.ac.at/

[US-EUMarch06a] *Large ICT-based Infrastructures and Interdependencies: Control, Safety, Security and Dependability*, Joint US-EU Workshop, 16-17 March 2006, Washington, DC, http://trust.eecs.berkeley.edu/euus/.

[US-EUMarch06b] *Terms of Reference* (for [US-EUMarch06a], http://trust.eecs.berkeley.edu/euus/euus_lci.pdf

[UROME] http://www.let.uniroma1.it/

[WMB05] Felix Wu, Khosrow Moslehi, and Anjan Bose. "Power System Control Centers: Past, Present, and Future". *Proceedings of the IEEE*, 93(11), November, 2005, 1890–1908.

APPENDIX: EC Funding Process

In the US, the funding process is relatively straightforward and understandable. Research projects are typically awarded with durations of between two to three years. Funding agencies such as the National Science Foundation (NSF) or the Defense Advanced Research Projects Agency (DARPA) have a relatively large degree of latitude in deciding the research programs which they will fund, though there are certainly sometimes political considerations and occasionally a program mandated (*de jure* or at least *de facto*) by the US Congress. Research programs are initiated each year.

In Europe the research funding situation is very different, and in many ways more complicated and potentially confusing to an outsider. The EC has much longer program lengths, often under the umbrella of a framework programme (FP). FPs have been used to organize most EC research since 1984. Each FP has run for five years, with the last year of a FP overlapping with the first year of the next one. The current FP is FP6, which runs until the end of 2006. FP7 will break this pattern, however. It will start at the beginning of 2007, but run for seven years. The total funding likely for FP7 is in the neighborhood of 70 billion[1] euros (85 billion dollars at recent rates).

In practice, there is little continuity between FPs, for a number of reasons. The next FP is being defined in the middle of the previous FP. Additionally, just like in the US (or presumably anywhere), a given topic may die if a high-level funding manager who was its advocate leaves the agency.

The EC also funds research outside of the FP mechanism, but the authors have no firsthand experience with them and thus their discussion is outside the scope of this report.

It is presumably not easy for a funding agency in the US to decide on research areas to fund. It is much more difficult for the EC to do so, however, given that it comprises many nations with a diversity of economies, cultures, and political heritages. To help decide on the foci of an FP, the EC uses *Preparatory Action* to help identify, define, and prioritize possible research areas. A Preparatory Action might include a budget in the neighborhood of €15M, and would fund two kinds of projects: Supporting Activity and Small Projects. A *Supporting Acvitivy* is a project that helps define roadmaps, helps connect colleagues, and/or looks towards standardization issues. *Small Projects* are feasibility demonstrations to show what is possible, and often include demonstrations of interoperability of technologies. Additionally, there is a *Group of Personalities* with a broad range of backgrounds that is appointed to brainstorm "outside the box" of the current FP context which helps provide valuable input to the formulation of the research areas for the new FP.

An example of a Preparatory Action is the recent one for security research. An overview of it can be found at [SEC-PREP-OVER], projects funded under it can be found at [SEC-PREP-PROJ1] and [SEC-PREP-PROJ2], and its report from its group of personalities can be found at [SEC-

[1] Given the intended primary audience of this document—US researchers and government employees—here we use the term *billion* to mean the American meaning (one thousand million), rather than in the British meaning (one million million).

PREP-PERSON]. The general EC security research overview page can be found at [SEC-HOME].

There are a number of different kinds of funding mechanisms within an FP, with different sizes, scopes, and partnering requirements. These include:

- **IP** An *Integreated Project* (IP) integrates basic and foundational research, component research, systems engineering and integration. It typically also involves training activities, involves SMEs (Small and Medium Enterprises, with 100–500 employees) for component development, and often considers the participation of technology brokers. An IP is typically 60/40 applied/theory, depending on the background of the project lead. It typically has 15–25 partners with a 50/50 academic/industrial breakdown. An IP typically runs 3–4 years and has a budget of €8–12M.
- **STREP** A *Specific Targeted Research Project* (STREP) explores emerging technologies or alternative approaches opening new projects in the field. It is often the best research vehicle for academic researchers in Europe, with a 70/30 split between theory/applied, depending somewhat on the background of the project lead. A STREP typically has 4–8 partners, a duration of 2.0–3.5 years, and a budget of €1–4M.
- **NoE** A *Network of Excellence* (NoE) project creates virtual research centers on specific scientific domains. They involve both universities and companies. They are typically about 20% research and the rest community building (the assumption here is any significant research done by the partners will be done through partner internal funding). They are not primary vehicles for academic research; their benefits are in building technical communities, from which coalitions for projects can emerge. An NoE typically lasts 3.0–3.5 years, has 25–30 partners, and a budget of €4–5M.
- **FET** A *Future Emerging Technologies* (FET) project is similar to a STREP in scope, but it is for very forward-thinking pre-proposal ideas that will flesh out ideas that can lead to a full proposal.
- **SSA** A *Specific Support Action* (SSA) project is a mechanism that is often used for an EC project manager to help define a program that should be funded in the next round of proposal solicitaions. It has great flexibility: there are few formal guidelines on the number and type of partners and other characteristics of the project. Typically, though, they will involve 4–6 partners, last 1–2 years, and have a budget of €0.3–1.0M.
- **CA** A *Coordinated Action* (CA) project is used for community building and the definition of research agendas. It has the same kinds of flexibility and typical characteristics as an SSA project.

From this set, the IP and STREP are the most commonly used mechanisms for funding projects that are involving academic research. However, due to their flexibility, the SSA and CA may be the best vehicles for helping define concrete possibilities for EC-US collaboration in CIP.