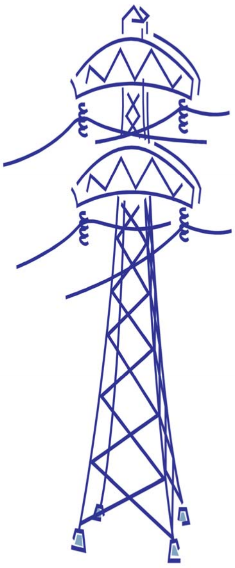
JRC Scientific and Technical Reports

Current efforts concerning ICT security of the power grid

Alberto Stefanini, JRC - IPSC
Andrei Z. Morch, SINTEF Energy Research
Giovanna Dondossola, CESIRicerca
Geert Deconinck, Katholieke Universiteit Leuven
Paul Friessem, Fraunhofer-SIT



GRID
A coordination action on ICT vulnerabilities of power systems
and the relevant defence methodologies

EUR 23268 EN - 2008

EUROPEAN COMMISSION

Institute for the Protection
and Security of the Citizen

The Institute for the Protection and Security of the Citizen provides research-based, systems-oriented support to EU policies so as to protect the citizen against economic and technological risk. The Institute maintains and develops its expertise and networks in information, communication, space and engineering technologies in support of its mission. The strong cross-fertilisation between its nuclear and non-nuclear activities strengthens the expertise it can bring to the benefit of customers in both domains.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Alberto Stefanini
Address: TP 210 I-21020 Ispra (VA)
E-mail: alberto.stefanini@jrc.it
Tel.: +39.0332.789752
Fax: +39.0332.789576

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC 43772

EUR 23268 EN
ISSN 1018-5593
Luxembourg: Office for Official Publications of the European Communities

Printed in Italy

GRID

A coordination action on ICT vulnerabilities of power systems and the relevant defence methodologies

Report

on

Current efforts concerning ICT security of the power grid

Authors: Alberto Stefanini, JRC – IPSC
Andrei Z. Morch, SINTEF Energy Research
Giovanna Dondossola, CESIRicerca
Geert Deconinck, Katholieke Universiteit Leuven
Paul Friessem, Fraunhofer-SIT

Date of Preparation: January 24, 2008

SUMMARY

GRID is a Coordination Action funded under the Trust and Security objective of the IST Programme of the 6th Framework to achieve consensus at the European level on the key issues involved by power systems vulnerabilities, in view of the challenges driven by the transformation of the European power infrastructure and ICT integration. GRID wants to assess the needs of the EU power sector on these issues, so as to establish a Roadmap for collaborative research in this area.

The present report provides a survey on current efforts somewhat related to the objectives of GRID. Similar to GRID, a number of European and US endeavours have attempted in recent years to draw a Road Map so as to coordinate efforts concerning energy transport/distribution research and CIP. Five of these Road Mapping projects appear related to GRID:

- the US-Canada Roadmap to Secure Control Systems in the Energy Sector, resulting from collaborative work between governments (sponsoring the activity) and industry with an active involvement and leadership of energy asset owners and operators;
- CI^{2}RCO, a Co-ordination Action co-funded under the IST priority of the 6th Framework. CI^{2}RCO established a European taskforce to encourage a co-ordinated approach for research and development on Critical Information Infrastructure Protection;
- SmartGrids, a European Technology Platform involving industrial stakeholders, conceived by DG Research with the support of FP 5 and 6 research clusters. SmartGrids is to formulate a vision for the development of Europe's electricity networks looking towards 2020 and beyond, in view of the main drivers of the power sector.
- RELIANCE, a coordination action among European Transmission System Operators, utilities and energy research, aimed at establishing collectively a research roadmap and assessing its implementation risks.
- ERMINE, a coordination action whose objective is to provide the recent and present scenario of the electricity Research and Technology Development (RTD) efforts in Europe (*map*), as well as to indicate specific RTD needs of the European electricity sector in the next 20-25 years (*road map*).

In addition to the above, there are many specific EU and national research projects pertaining to the area of Critical Information Infrastructure Protection (CIIP). This report provides a summary of the survey made in 2006 within GRID by A.Z. Morch [20]. Moreover the report provides an overview of current standardisation activities in the area, based on a previous survey by some of the authors [21]. Recent and current EU and national projects in the area are assessed in order to establish their relevance to the objectives of GRID – more specifically the ones identified within the recently delivered draft GRID Road Map.

1 INTRODUCTION

EU power systems are undergoing an in-depth restructuring so as to cope with the enlargement, open access and the progressive integration of the EU electricity market and intensification of cross border trade. Emergent control technologies, like wide area monitoring and adaptive controls, appear to be potentially useful for dealing with the new situation especially regarding monitoring. But their full application will demand a new approach to the design and system operation. Indeed, their integration within existing control infrastructures and practices is a real challenge. These factors contribute to increase power system vulnerabilities, in a worldwide scenario where malicious threats against large and complex infrastructures are intensifying.

Since the inception of the issue in the early nineties, several CIP related efforts have tried to provide general frameworks for investments to protect critical national infrastructures. Some of these endeavours took the approach of Road Maps, i.e. broad and far sighted plans to increase infrastructure resilience, identifying mid and long term objectives (10-20 years) and relevant measures. Aside measures to strengthen the physical and cyber robustness of CIP based on available technology, these Road Maps included generic and specific R&D efforts to improve infrastructure dependability, resilience and survivability. This report provides a survey of the most recent and contemporary road mapping efforts in Europe and the US somewhat concerned with critical infrastructure protection. Recent and current EU and national projects in the area are also assessed in order to establish their relevance to the objectives of GRID – more specifically the ones identified within the recently delivered draft GRID Road Map. Recent and current EU and national projects in the area are also assessed in order to establish their relevance to the objectives of GRID, and a gap analysis is attempted.

1.1 The US-Canada Roadmap to Secure Control Systems in the Energy Sector

The US-Canada Roadmap to Secure Control Systems in the Energy Sector (USCR) [www.controlsystemsroadmap.net/] was issued in January 2006 as a result of a collaborative work between governments (sponsoring the activity) and industry with an active involvement and leadership of energy asset owners and operators. A distinctive feature of this collaborative effort is the active involvement and leadership of energy asset owners and operators in developing the Roadmap content and priorities. The Roadmap synthesizes expert input from the control systems community, including owners and operators, commercial vendors, national laboratories, industry associations, and government agencies. The Roadmap project was funded and facilitated by the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability in collaboration with the U.S. Department of Homeland Security's Science and Technology Directorate and the Energy Infrastructure Protection Division of Natural Resources Canada. Aimed at improving the power system cyber security through a coherent plan to be used by industry and government as a template for action, the Project purposes were to define a consensus on needs, produce a comprehensive plan and guide efforts by industry, academia and government within the next ten years.

The US map covers the whole energy sector (including electricity, oil and gas infrastructures) with a limited reference to distributed generation, addresses issues related to both legacy upgrades and new generation designs by identifying relevant activities spanning over R&D, testing, best practices, training and education, policies, standards and protocols, information sharing.

The vision expressed in the US map is that "*in 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function*".

The US road map contains a structured set of priorities that address specific control systems needs within the next 10 years. The following four pillars have been distinguished to reach the envisioned objective:

- *Measure and assess security posture*
- *Develop and integrate protective measures*
- *Detect intrusion and implement response strategies*
- *Sustain security improvements.*

Per each of the pillars above a strategy has been developed and illustrated by means of a table including challenges, near- mid- and long-term milestones and priorities where priorities are associated to the following needs:

- *Identifying strategic risks*
- *Legacy systems*
- *Security tools and practices*
- *New Control system architecture.*

Finally the US road map outlines the main implementation steps that will result in a industry-managed process for guiding and aligning existing efforts, addressing critical needs and gaps, launching control systems projects, coordinating and managing the roadmap project.

The US Road Map is the closer in scope to the GRID one among those considered in this review. However there are important differences pertaining sponsorship, participants, scope, aim, purpose and timeframe in between the two Road Maps:

- **Sponsorship:**
  - USCR is directly sponsored by the US and Canada governments in a joint effort,
  - GRID is partly funded by the Commission through the EU framework R&D programme.
- **Participants:**
  - USCR is a collaborative work between industry and government with active involvement and leadership of energy asset owners and operators.
  - GRID is lead by its research partners, and performs consultation actions toward the industry. Member state governments are not directly involved. Stakeholders are directly involved in an advisory role, through the Stakeholders Advisory Board.
- **Scope:**
  - USCR i) covers the whole energy sector ii) addresses both legacy upgrades and new generation designs iii) includes activities of R&D, testing, best practices, training and education, policies, standards and protocols, information sharing iv) makes limited reference to distributed generation.
  - GRID i) covers the electricity domain only (no oil and gas) ii) stresses on legacy updates more than new generation designs iii) mostly focuses on R&D activities iv) stresses on the impact of distributed generation on control architectures.
- **Aim:**
  - USCR is aimed at improving cyber security through a coherent plan to be used by industry and government as a template for action.
  - GRID is aimed at improving cyber security through a research roadmap which by its nature may impact on cyber security in an *indirect* way and in a *longer* term.
- **Purpose:** although both maps are comprehensive plans based on consensus, the USCR aspires to guide coordinated efforts by industry, academia and the national governments involved.
- **Timeframe:** in accordance with their different aim and scope, the two Road Maps have a different time frame: - USCR: 10 years (2005-2015) - GRID: 15 years (2007-2022).

1.2 The Critical Information Infrastructure Research Co-ordination project (CI^{2}RCO)

The Critical Information Infrastructure Research Co-ordination (CI^{2}RCO) project [www.ci2rco.org], a two-year project which started in 2005, was a so called Co-ordination Action co-funded under the Information Society Technologies (IST) Priority of the 6th Framework Programme by the European Commission. The project addressed the creation and co-ordination of a European taskforce to encourage a co-ordinated approach for research and development on CIIP. The main objective of the CI^{2}RCO project was thus to create and co-ordinate a European Taskforce:

- to encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection,
- to establish a European Research Area (ERA) on CIIP as part of the larger IST strategic objective to integrate and strengthen the ERA on dependability and security, and
- to support CIIP awareness and actions in the former EU-25, Associate Candidate Countries (ACC)2 as well as the EU Associated States (Norway, Switzerland, and Israel).

Though the project also produced a gap analysis of existing CIIP R&D programmes at regional, national an EU level, which was done in cooperation with the R&D community and the stakeholders (including electric power production and distribution), its major goal was to establish a European CIIP R&D Agenda, and the project didn't focus on sector-specific gaps or needs, but on cross-sector CIIP issues. So the findings and recommendations of CI2RCO are a valuable background when you consider how to make the GRID roadmap happen, and many of the general results of CI2RCO can be supported from the in-depth experience in the closer GRID sector, but in practice there is little overlapping.

1.3 The European Technology Platform for the Electricity Networks of the Future (SmartGrids)

SmartGrids [www.smartgrids.eu/] is a European initiative involving industrial stakeholders, organised as a so-called Technology Platform. The initial concept and guiding principles of the Technology Platform were developed by the European Commission Directorate General for Research, with the support of research clusters within FP 5 and 6. SmartGrids began its work in 2005. Its aim is to formulate and promote a vision for the development of Europe's electricity networks looking towards 2020 and beyond, in view of the main drivers of the power sector:

- to support the EU environmental policy
- to provide response to the growing demand for electricity in a landscape where European energy markets are liberalized
- to cope with the increasing role of distributed generation and ensure interoperability of European electricity networks

Its main objectives are:

- to develop a shared vision for the future which encourages the engagement of multiple, independent parties
- to identify research needs and build support for an increased public and private research effort on electricity networks
- to align ongoing RTD projects and new European, national and regional programmes on electricity transmission and distribution systems
- to draw conclusions and recommendations for follow-up actions and implementation of the strategic research agenda and deployment plan.

The platform is organized so as to be *open and accessible*, allowing the participation of all active stakeholders, and to be *user-centric*. It is steered and monitored by an Advisory Council (AC), nominated in May 2005, which provided guidance on the definition, initiation and putting in place of the structure, procedures and work programme. The AC set up an Executive Group which proposed the initiatives that led the Platform in its initial steps. Now the operational structure of the platform is based on the Mirror Group, whose current members include representatives from 19 countries, thus enabling the involvement of EU Member States, candidate countries and associate countries.

SmartGrids has achieved a shared Vision, whose main elements are:

- *sustainability, competition, security of supply*
- *flexibility:* fulfill customers needs
- *accessibility* to all network users, particularly RES and high efficiency DG with zero or low CO2 emissions
- *reliability:* assuring and improving Quality of Supply and be resilient to hazards and uncertainties
- *economics:* best value through innovation, efficient energy management, level the playing field, encourage competition while coping with EU and national market regulations

in a landscape where key future requirements are:

- customers are part of the "network-loop", both producer and consumer = "prosumer"
- utilities must provide real-time price information (smart meters)
- regulators must provide adequate investment and reward incentives
- the system will have to integrate millions small scale generators
- bulk power and small scale generators must coexist
- demand and supply balancing solutions are required

These requirements demand for a Future Network Vision whose key concepts are:

- **Microgrids:** LV networks with DG sources, local storage, controllable loads, automatic islanding

- **Virtual Utilities**: to configure distributed generation resources and deliver differentiated power quality at the connection point
- **Internet model:** the customer must be in control

The SmartGrids Research Area (SRA) includes five main areas:

1) Smart Distribution Infrastructure (Small Customers & Network Design)
2) Smart Operation, Energy Flows & Customer Adaptation (Small Customers & Networks)
3) SmartGrid Assets and Asset Management (T&D)
4) European Interoperability of SmartGrids (T&D)
5) Smart Grids Cross-Cutting Issues and Catalysts

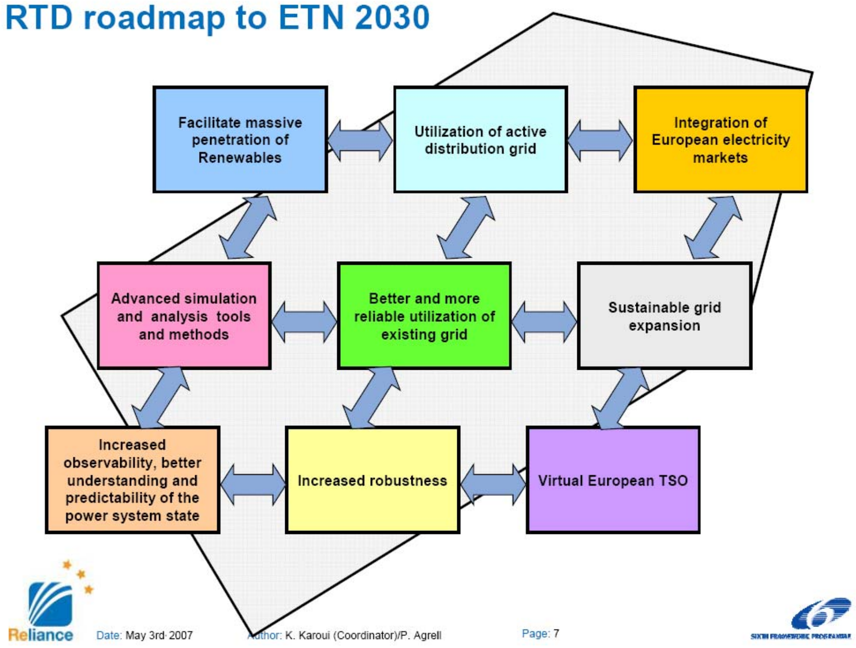
Within the SRA landscape three specific research themes, RT 3.2: **Transmission networks of the future: new architectures & new tools,** RT 4.3. **Architectures and tools for operations, restorations & defence plans,** and RT5.2, **The networks of the future –Information and Communication**, appear to be more specifically concerned with issues related to ICT vulnerability.

1.4 The RELIANCE action

"CooRdination perspectives of the European transmission network research activities to optimise the reLIAbility of power supply, usiNg a systemiC approach, involving growing distributed generation and renewable energy markEts" - in short RELIANCE – is a coordination action elaborated by eight European Transmission System Operators (TSO), one Power Producer, one Distribution System Operator (DSO) and several Research Centres (www.ca-reliance.org).

One of the objectives of the project was to design collectively a research roadmap and assess its implementation risks. This research roadmap, towards a European Transmission System, targets the time horizon of 2030.

According to www.ca-reliance.org, the RELIANCE roadmap is pictured in 9 domains.



RTD roadmap to ETN 2030

Facilitate massive penetration of Renewables

Utilization of active distribution grid

Integration of European electricity markets

Advanced simulation and analysis tools and methods

Better and more reliable utilization of existing grid

Sustainable grid expansion

Increased observability, better understanding and predictability of the power system state

Increased robustness

Virtual European TSO

Reliance Date: May 3rd 2007 Author: K. Karoui (Coordinator)/P. Agrell Page: 7

Figure 1 The Reliance Road Map [Source : Reliance presentation to Commission, **www.ca-reliance.org**]

Each of these nine boxes has been developed into a fully elaborated set of objectives, which will be released at the project's final conference in Ljubljana (21/9/2007). This roadmap has been refined over time as in the following figure.

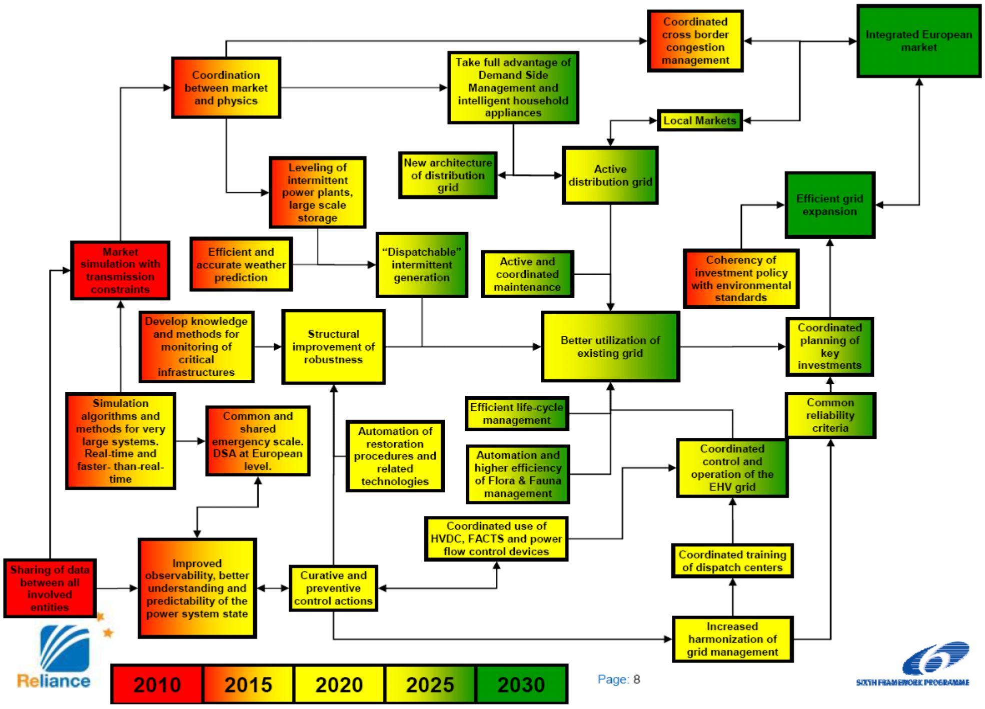

Coordinated cross border congestion management
Integrated European market
Coordination between market and physics
Take full advantage of Demand Side Management and intelligent household appliances
Local Markets
Leveling of intermittent power plants, large scale storage
New architecture of distribution grid
Active distribution grid
Efficient grid expansion
Market simulation with transmission constraints
Efficient and accurate weather prediction
"Dispatchable" intermittent generation
Active and coordinated maintenance
Coherency of investment policy with environmental standards
Develop knowledge and methods for monitoring of critical infrastructures
Structural improvement of robustness
Better utilization of existing grid
Coordinated planning of key investments
Simulation algorithms and methods for very large systems. Real-time and faster- than-real-time
Common and shared emergency scale. DSA at European level.
Automation of restoration procedures and related technologies
Efficient life-cycle management
Automation and higher efficiency of Flora & Fauna management
Common reliability criteria
Coordinated control and operation of the EHV grid
Coordinated use of HVDC, FACTS and power flow control devices
Coordinated training of dispatch centers
Sharing of data between all involved entities
Improved observability, better understanding and predictability of the power system state
Curative and preventive control actions
Increased harmonization of grid management
Reliance
2010
2015
2020
2025
2030
Page: 8
SIXTH FRAMEWORK PROGRAMME

Figure 2 The Reliance areas of interest [Source : Reliance presentation to Commission, www.ca-reliance.org]

While the focus of the Reliance roadmap is related to many different aspects (including economic ones) of the transmission systems of the future, several elements from the Reliance roadmap are very parallel to the Grid roadmap. Some examples include :

- simulation and analysis tools
- addressing occurrences of multi-contingencies
- methods for monitoring critical architectures
- improved cyber security
- new architectures for distribution grids
- autonomous microgrids

1.5 Electricity Research Road Map In Europe (ERMINE)

The ERMInE project (http://www.ermine.cesiricerca.it) is a co-ordination action supported by the European Commission under the 6th R&D Framework Programme. The general objective of ERMInE is to provide the recent and present scenario of the electricity Research and Technology Development (RTD) efforts in Europe as well as to indicate specific RTD needs of the European electricity sector in the next 20-25 years. The main project activities are:

- Collection of data on the structure and characteristics of the existing electricity system of each European country
- Collection of data on RTD efforts (subjects, funding, performers …) in the recent and present electricity sector of EU25
- Collection of data on foreseen trends of RTD priorities and efforts for the electricity sector of EU25 in the next 20-25 years
- Definition of a Map (present situation of electricity RTD in Europe) and a Roadmap (possibilities of evolution of the electricity sector), according to the collected information

These activities are carried out by means of questionnaires, interviews, workshops, focused meetings and symposia, addressed to European public regulators, utilities/companies, equipment manufacturers, network operators, research institutes and associations.
The overall resulting data are collected in a digital databank, organised in national sections, and can be analysed according to appropriate selection and filtering criteria.

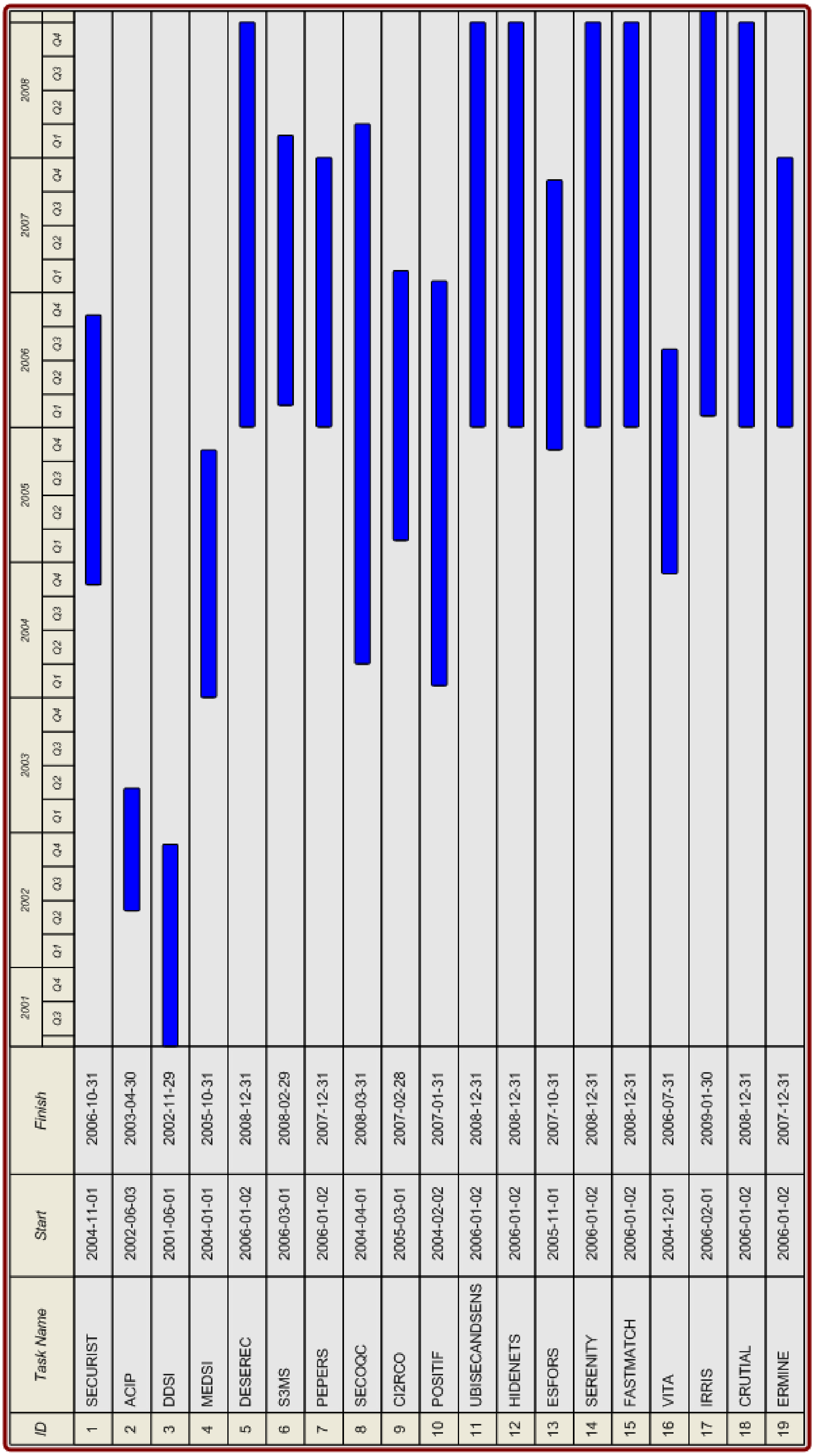
2 EUROPEAN RESEARCH AND DEVELOPMENT PROJECTS

The following chapter gives a brief description of European R&D projects related to the CIIP-area[1]. Recent EU Networks of Excellence and Platforms are not included in this survey, because they were overviewed in Chapter 2. Hence the chapter includes two sections:

- Generic projects – projects addressing general ICT security issues as for examples cryptography, security in data communication, operation systems (OS) etc.
- Applied projects – projects addressing concrete security issues in the Power Industry

The overall scale of the CIIP-related research in the EU was reinforced after initiation of Information Society Technology Framework Program 6 (IST-FP6). The major part of the relevant projects belongs to a specific area: "Towards a global dependability and security framework" under this program as it is illustrated in [20].

[1] Description of the projects is based on information from European Community Research and Development Information Service (CORDIS). CORDIS usually provides very long web links to the projects' descriptions. Therefore in order to find the projects description at CORDIS, the readers are advised to search on http://cordis.europa.eu/search using a project's acronym.



ID	Task Name	Start	Finish
1	SECURIST	2004-11-01	2006-10-31
2	ACIP	2002-06-03	2003-04-30
3	DDSI	2001-06-01	2002-11-29
4	MEDSI	2004-01-01	2005-10-31
5	DESEREC	2006-01-02	2008-12-31
6	S3MS	2006-03-01	2008-02-29
7	PEPERS	2006-01-02	2007-12-31
8	SECOQC	2004-04-01	2008-03-31
9	CI2RCO	2005-03-01	2007-02-28
10	POSITIF	2004-02-02	2007-01-31
11	UBISECANDSENS	2006-01-02	2008-12-31
12	HIDENETS	2006-01-02	2008-12-31
13	ESFORS	2005-11-01	2007-10-31
14	SERENITY	2006-01-02	2008-12-31
15	FASTMATCH	2006-01-02	2008-12-31
16	VITA	2004-12-01	2006-07-31
17	IRRIS	2006-02-01	2009-01-30
18	CRUTIAL	2006-01-02	2008-12-31
19	ERMINE	2006-01-02	2007-12-31

Figure 1 Comparative time schedule for the European projects

2.1 Generic projects, addressing general information security issues

Security IST Projects cluster support (SECURIST)

SecurIST was to deliver a Strategic Research Agenda for ICT Security and Dependability R&D for Europe. It identified priorities for Europe, mechanisms to effectively focus efforts on those priorities, and instruments for delivering on those priorities and a coherent time frame for delivery.

Reference: http://www.ist-securist.org/

Analysis and Assessment for critical infrastructure protection (ACIP)

The goal of ACIP was to determine how protection of critical infrastructures can be analysed and assessed by modelling and simulation (M&S) and to provide a roadmap for the development and application of modelling and simulation, gaming and further adequate methodologies and tools.

References: http://www.iabg.de/acip/index.html

Dependability Development Support Initiative (DDSI)

The objective of DDSI was to support the development of dependability policies across Europe and across sectoral boundaries. It aims to establish networks of interest, to provide baseline data and to develop policy roadmaps. These products will support policy-supporting activities by European institutions and by public and private sector stakeholders across the EU, in Accession States and in partner nations including the USA.

References: http://www.ddsi.org

Management Decision Support for Critical Infrastructures (MEDSI)

MEDSI was to develop a web-based integrated set of software services as a tool to enhance the capabilities of crisis planners and crisis managers in both private and governmental organizations. The system will be used by users from general security area, as well as, environmental protection, utilities management, airports and seaports, healthcare, transports, roads, energy plants, borders control etc.

Reference: http://www.medsi.org

Security of Software Services of Mobile Systems (S3MS)

S3MS creates a framework and a technological solution for trusted deployment and execution of communicating mobile applications in heterogeneous environments. S3MS would enable the opening of the software market of nomadic devices (from smart phones to PDA) to trusted third party applications beyond the sandbox model, without the burden of roaming trust infrastructure but without compromising security and privacy requirements.

Reference: http://www.s3ms.org

Mobile Peer-to-Peer Security Infrastructure (PEPERS)

PEPERS works on a reliable platform with high-level support for the design, development and operational deployment of secure mobile peer-to-peer applications for future AmI environments. The project will address issues related to security, privacy, trust and access control in mobile peer-to-peer (p2p) systems by proposing a relevant framework architecture.

Reference: http://www.pepers.org/

European Security Forum for Web Services, Software and Systems (ESFORS)

ESFORS is a Coordination Action that aims at bringing together the European stakeholders for security and dependability information and communication technologies to address the security and dependability requirements of emerging software service platforms. This emergence of open service platforms such as web services provides major opportunities to position the European software industry at the heart of the emerging information society.

Reference: http://www.esfors.org/

Highly dependable ip-based Networks and services (HIDENETS)

HIDENETS develops and analyses end-to-end resilience solutions for distributed applications and mobility-aware services in ubiquitous communication scenarios. The HIDENETS solutions are essential for the deployment of future applications: the use of off-the-shelf components and wireless communication links will dramatically decrease the costs of market entry and hence make such ubiquitous scenarios commercially feasible.

Reference: http://www.hidenets.aau.dk/

Framework architecture to semantically integrate advanced threat detection and security protection at ultra-high speeds (FASTMATCH)

The project works on an agent-oriented layered architecture to enable the delivery of multiple pattern-based and behaviour-based scanning and filtering functions at very high speeds. The objectives are to provide a framework for the concurrent operation of reactive and proactive security algorithms, to deliver algorithmic enhancements for pattern recognition and behaviour-based detection schemes and rule sets for more efficient alarm management and root-cause analysis.

Reference: http://www.fastmatch.org/

Resilience for survivability in IST (ReSIST)

ReSIST integrates research on Dependability, Security, and Human Factors in order to create a coherent set of research activities aimed at ensuring that future "ubiquitous computing systems" (the immense systems of ever-evolving networks of computers and mobile devices which are needed to support and provide Ambient Intelligence (AmI)) will have the necessary resilience and survivability.

Reference: http://www.laas.fr/RESIST/

2.2 Applied projects, addressing specific Critical Infrastructure Protection issues in Power sector

Vital Infrastructure Threats and Assurance (VITA)

The VITA project aimed at delivering assessment on the threats to and assurance and protection of highly networked infrastructures, most of which are operating trans-nationally, and disruption of which is critical to Europe’s security. The project has provided: methods to raise awareness on the need for vital infrastructure protection, an approach on methods, tools and technologies for the protection improvement and a demonstrator experiment by a scenario exercise with focus on energy.

Reference: http://vita.iabg.eu/

Integrated Risk Reduction of Information-based Infrastructure Systems (IRRIIS)

The extensive use of information and communication technologies has pervaded all infrastructures, making them increasingly interdependent and more vulnerable. IRRIIS analyses, models and simulates the dependencies between ICT-based infrastructures and provides appropriate middleware technology to increase dependability and resilience of ICT-based critical infrastructures.

Reference: http://www.irriis.org/

Critical Utility Infrastructure Resilience (CRUTIAL)

CRUTIAL, CRitical UTility InfrastructurAL Resilience, addresses networked ICT systems for the management of the electric power grid, where control systems need to be connected with information infrastructures via Internet. The project approach resides in modelling interdependent infrastructures taking into account the multiple dimensions of interdependencies, and attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks.

Reference: http://crutial.cesiricerca.it/

3 NATIONAL RESEARCH AND DEVELOPMENT PROJECTS

3.1 Belgium

Reaching for 100% Reliable Electricity Services: Multi-system Interactions and Fundamental Solutions (GOA)

GOA is a national project, carried out at Katholieke University Leuven in Belgium and funded by the Research Council of the university. The project aims for a basic research study of the limits to reliable power supply, to fundamentally analyse shortcomings in today's methods and tools, and to indicate ways for totally new and fundamental solutions for the future.

URL: http://www.kuleuven.ac.be/research/researchdatabase/project/3E05/3E051043.htm

3.2 Italy

Ricerca di Sistema (RdS)

RdS is an Italian Research Programme to perform research and development activities aimed to improve the economics, security and quality of the Italian electric system. The main objective is to devise solutions to practical problems, in view of the power system evolution and the scientific-technological progress, so as to sustain the changes dictated by international agreements (Kyoto). This Research Programme is structured in projects participated by the major research operators in the electrical field and academics, whose results are made public in form of reports or published papers (in Italian). More than 70 universities and research centres were involved in Italy and abroad. Until 2005 CESI (Centro Elettrotecnico Sperimentale Italiano) had been appointed to manage the funds assigned to the projects.

The Programme covers a wide-scope area of research in power generation, transmission, distribution and final uses, renewable and dispersed energy sources, nuclear, hydrogen, grid development, power system control, power transmission technologies, power saving and quality. Specific activities focus on protection techniques for both accidental and intentional threats of different nature (environmental, atmospheric, physical, logical) and on reducing the environmental impact of power installations. Of specific interest for GRID are the projects presented in Table 1.

Table 1 Overview of CIP related RdS projects

Acronym	Italian title	English title	Time-frame
EXTRA	Sviluppi del mercato liberalizzato dell'energia elettrica in Italia e sua integrazione nel mercato elettrico Europeo	Developments of the liberalised electric market in Italy and its integration in the European electric market	2003-2005
GENDIS 21	La generazione distribuita per il miglioramento della qualità del servizio elettrico e dell'ambiente	The distributed generation for the improvement of the power quality service and of the environment	2003-2005
NORME	Sviluppo di norme a sostegno delle	Development of norms to support	2003-2005

	esigenze del sistema elettrico Nazionale	the needs of the national electric system	
RETE 21	Lo sviluppo e l'esercizio delle rete elettrica italiana nel XXI secolo	The development and the operation of the Power Grid for the 21st Century	2003-2005
SENNA	Sensoristica innovativa e nanomateriali per il sistema elettrico	Innovative sensors and nanotechnologies for the power system	2003-2005
SISET	Sicurezza degli impianti del sistema elettrico e interazione con il territorio	Security of the power system plants and interaction with the environment	2003-2005
CATERINA	Aumento della capacità di trasporto della rete	Increasing the grid transport capacity	2000-2003
COMUNICA	Comunicazione tra e nei sistemi elettrici	Communication intra and inter electrical systems	2000-2003
ENTRADE	Energy Trading: modelli e funzionamento dei mercati liberalizzati del'energia	Energy trading: models and mechanisms of the liberalised markets	2000-2003
EVORE	Evoluzione della rete elettrica	Evolution of the electric power grid	2000-2003
SICURE	Funzionamento in sicurezza del sistema elettrico	Secure operation of the electric system	2000-2003
SISIGEN	Sicurezza del sistema elettrico	Electrical system security	2000-2003

Reference: http://www.ricercadisistema.it/

3.3 Norway

Protection of the Society / Beskyttelse av Samfunnet (BAS)

The project [16] focused on vulnerability of the national power system in the perspective of the more serious threats as intentional man-made attacks and natural disasters in a national security context. Based on results of the study, the Norwegian Defence Research Establishment (FFI) recommended a minimum package of measures, emphasising ICT security, increased ability to re-establish power supply after outages, robustness of important objects and nodes, emergency planning and training. As a result of the study, the Norwegian Defence Research Establishment (FFI) recommended a minimum package of measures with emphasis on:

- Information and communication technology security
- Increased ability to re-establish power supply after outages
- Robustness of important objects and nodes
- Emergency planning and training

It was also pointed out that the production margins in the power supply system must increase with needs for investments in new constructions, import capacity and energy saving measure. However, new constructions in power plants and lines are not an easy task in the modern Norway, with a lot of challenges from the pure cost to environmental issues.

Reference: http://www.nve.no/modules/module_109/publisher_view_product.asp?iEntityId=5782

Vulnerability of the Nordic Power System

This study was funded by the Nordic Council of Ministers and carried on by SINTEF Energy Research in 2003 . The main objective of the study was to:

- Identify incidents, situations and scenarios leading to critical or serious consequences to the society and the power system
- Identify barriers to handle and reduce the vulnerability
- Identify possible countermeasures and actions to handle and reduce the vulnerability

The Results of the study are presented in the final report [18] and in its executive summary [19].

3.4 USA

GridWise™ Alliance

The GridWise Alliance is a consortium of public and private stakeholders who are aligned around a shared vision of an electric system that integrates the infrastructure, processes, devices, information and market structure so that energy can be generated, distributed, and consumed more efficiently and cost effectively; thereby achieving a more resilient, secure and reliable energy system. The Alliance provides a forum where members representing a broad range of interests in the electricity sector can meet, exchange ideas, and work cooperatively on a common set of issues, with the goal of moving our industrial-age electric grid into the information age. In addition, the Alliance provides its members with opportunities to interact with senior policy makers on both the US federal and state level. In their 2004 Memorandum of Understanding, the GridWise Alliance and the U.S. Department of Energy agreed to work together to realize the vision of a transformed national electricity grid.

URL: http://www.gridwise.org/

Team for Research in Ubiquitous Secure Technology (TRUST)

The Team for Research in Ubiquitous Secure Technology (TRUST) is a partnership between industry and academia devoted to the development of a new science and technology that will radically transform the ability of organizations (software vendors, operators, local and federal agencies) to design, build, and operate trustworthy information systems for their critical infrastructures. The major technical goal of TRUST is composition and computer security for component technologies. The role of the testbeds will be to integrate and evaluate technologies in specific and realistic systems, keep the research on track to answer societal objectives, and demonstrate the technologies for stakeholders in real systems.
Reference: http://trust.eecs.berkeley.edu

Trustworthy Cyber Infrastructure for the Power Grid (TCIP)

The TCIP NSF Cyber Trust Centre was created in August 2005 to address the challenge of how to protect the US power grid. The National Science Foundation (NSF) awarded $7.5 million over five years to the project, which will be led by the University of Illinois ITI team and also involve researchers at Cornell University, Dartmouth College, and Washington State University. The centre's intention is to improve significantly the way the power grid cyber infrastructure is built, making it more secure, reliable, and safe. TCIP is working to provide the fundamental science and technology needed to create an intelligent, adaptive power grid that can survive malicious adversaries, provide continuous delivery of power, and support dynamically varying trust requirements. The centre creates the necessary cyber building blocks and architecture, and by creating validation technology, quantifies the amount of trust provided by the proposed approach.

Reference: http://www.iti.uiuc.edu/tcip/

4 STANDARDS RELATED TO THE SECURITY OF CONTROL SYSTEMS

Most of the technologies used for control systems have shifted towards the adoption of off-the-shelf components used in general-purpose computation and communication: while taking advantage of the technical possibilities provided by the new ICT, power systems have inherited dangerous vulnerabilities. The benefits deriving from the adoption of standardized technologies accelerate the implementation of control systems and related communications without any guarantee of secure operation. Vulnerabilities due to design and technology flaws may be exploited by malicious antagonist actors, who can gain access to the systems through external and internal connections. These threats menace industry in the whole energy industrial spectrum, as their supervisory control and data acquisition systems (SCADA for short) are based on similar technologies and are deployed using analogous architectures. Standards might help in the protection of SCADA in different ways:

- Helping in setting a common conceptual basis between all stakeholders: operators, vendors, certifiers, authorities, etc.
- Supporting all engineering processes: from specification to procurement, and from operation to maintenance.
- Fostering the development of a market for security products and services, with verifiable levels of assurance.

Furthermore, there is a virtuous circle involving research, innovation and standardization processes:

- Research results are taken up by innovative products to be introduced in the market place;
- Innovation is fostered by standardization: the more standard approaches exist to secure product deployment, the faster is innovation take-up in the market place – i.e. technology deployment.

Standardization processes by their nature involve a uniformed knowledge management approach which clarifies needs, problems, issues, methodologies. Every standardization effort must starts with a glossary. But this helps to motivate and set the base for further research, oriented to solve the issues that knowledge management pointed out.

However, there is a time gap between the availability of standards and their application. Current efforts to consider security in SCADA standards are too recent for being sure about their effectiveness. In the meantime critical infrastructures and the process industry continue deploying SCADA systems. The situation is challenging, and by all accounts will continue to be so for the next decade – if not more. Industry is already waiting for standards that will not be ready in the next coming years. In the meantime information and communication technologies are being deployed with an ad-hoc approach to security, based on the restricted knowledge of each company.

According to a recent survey [21] several attempts exist to introduce cyber security standards in the SCADA sector. All main standard associations and stakeholder organizations appear to be involved, including ISO, NIST, IEC, NERC, CIGRE', API and AGA [*ibidem*].

In the following we focus on two approaches which appear to be centered on the power sector. Both are developed within IEC, the International Electrotechnical Commission. IEC [http://www.iec.ch/] is a standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies. These standards serve as a basis for creating national standards and as references for drafting international tenders and contracts. IEC's members include manufacturers, providers, distributors, vendors, consumers, users, all levels of governmental agencies, professional societies, trade associations, and standards developers from over 60 countries.

In 2004 the IEC Technical Sub-Committee **65C** (Industrial Process Measurement and Control – Digital Communications), through its working group **WG13** (Cyber Security), started to address security issues - within the IEC 61784 standard – for field buses and other industrial communication networks. Results of this work are outlined in part 4, entitled "Digital data communications for measurement and control – Profiles for secure communications in industrial networks".

The working group **WG10** of the IEC Technical Sub-Committee **65A** is working to extend this field level communication to address security standards across common automation networking scenarios. The standard being drafted as a result of this work is IEC 62443, entitled "Security for industrial process measurement and control – Network and system security". It is based on a modular security architecture consisting of requirement sets. These modules are mapped into ICS component and network architecture. The resulting requirements can then be formulated for use as the basis for Requests for Proposals for data communication standards, and security audits.

The IEC Technical Committee **57**, focused on Power Systems Management and Associated Information Exchange, set up the working group **WG15** - Data and communication security specifically devoted to the development of security standards for power system communication protocols defined by the other WGs of TC57 covering the telecontrol protocols, power line communications, power system IED communications, deregulated energy market communications, communication systems for distributed energy resources, hydroelectric power plants communications. Hence this effort appears more focused in scope on the power sector, while TC 65 A addresses all process sectors, and shows remarkable differences with respect to the previous one.

In conclusion, current standardization efforts concerning SCADA security appear to converge. The Process Control Systems Forum [https://www.pcsforum.org/] has established a common vocabulary and all current efforts, including IEC, CIGRE', ISA and AGA, are now converging towards that common set of definitions. The IEC TC 65 – WG 10 is leading together with the ISA SP-99, but it is likely that these latter will limit themselves in the future to issuing guidelines, leaving proper standardisation to the IEC TC 65 – WG 10. The time range to achieve a comprehensive cyber security standard about SCADA should be 3-5 years.

Divergence of some efforts (most remarkably TC 57) can be explained by the different - more peculiar - scope and mission. These two factors account for most of the differences a particular standard will add – e.g., in form of a qualifying language to a definition - to place particular emphasis on their scope of work. Specifically, WG 15 of TC 57 has a unique problem, in that they have to amend for cyber security specific communication protocols established quite long time ago, by 1995-96, and have to adapt to the original vision and terminology of the foundational documents. In conclusion, TC 57 is looking to more specific issues, peculiar of the electric power system sector. And cyber security requirements for some Transmission & Distribution equipment (e.g. Wide Area Monitoring and Protection) are far more stringent than the ones regarding SCADA in general.

5 POSITIONING OF CURRENT EFFORTS ON THE GRID ROAD MAP

In the following Tables the objectives defined by the GRID Road Map (left side) are matched with the objectives of the projects overviewed in chapters 3 and 4. A different colour identifies European, national and US projects.

Table 2 – Project positioning against GRID objectives in the Risk Assessment area

Risk & Vulnerability Assessment	
Near Term (0-3 years): *Initial studies*	
Identification/understanding of the classes, categories and characteristics of risks and vulnerabilities (present and forecasted)	**SECURIST** – *Establish and co-ordinate a European ICT Security & Dependability Taskforce* – *Drive the creation of an "ICT Security & Dependability Research strategy beyond 2010"* – *Leverage the knowledge base of existing/future ICT Security and Dependability researchers and projects* **MEDSI** – *Integration of Geographical Information Systems with DB, decision-support management and an auditory system to develop an advanced system that will be able to give support on decisions in a crisis* **FASTMATCH** – *Threat source identification and localization* – *Security management architectures to model and implement an intelligent intrusion detection system* **VITA** – *(Analyse) threat of Critical Infrastructures in Europe by natural disasters, manmade disasters and technical incidents* **Vulnerability of the Nordic Power System** - *Identify incidents, situations and scenarios leading to critical or serious consequences to the society and the power system* - *Identify barriers to handle and reduce the vulnerability* - *Identify possible countermeasures and actions to handle and reduce the vulnerability* **Beskyttelse av Samfunnet (BAS)** – *vulnerability of the national power system in the perspective of the more serious threats as intentional man-made attacks and natural disasters in a national security context*
Common methodologies for risk assessment and vulnerability analyses of integrated Power and ICT systems	**Vulnerability of the Nordic Power System** - *Identify incidents, situations and scenarios leading to critical or serious consequences to the society and the power system* - *Identify barriers to handle and reduce the vulnerability* - *Identify possible countermeasures and actions to handle and reduce the vulnerability*
Initial assessment of relevant methods and tools for risk and vulnerability analyses	**ACIP** - *How protection of critical infrastructures can be analysed by modelling and simulation* - *provide a roadmap for the development and application of*

modelling and simulation, gaming and further adequate methodologies and tools

Mid Term (3-8 yrs) : *Off line assessment tools and technologies: planning and design*

Off-line tools for analyzing the risk and vulnerability related to different hazards and threats (technical, human errors, malicious attacks, weather related, etc)
Assessment of defensive strategies and incident reporting

VITA

- *Protect such infrastructures via realistic scenario and crisis management simulation*

Long Term (8-15 yrs): *On line and Operational assessment*

Realization of operational tools for vulnerability assessment of components and systems, taking into account expected evolutions and scenarios

Table 3 – Project positioning against GRID objectives in the Controls area

Control Architectures and Technologies	
Near Term (0-3 yrs): *Crosscutting issues*	
Understanding interdependencies and cascading effects of ICT faults and scenarios	**ACIP** - *how protection of critical infrastructures can be analysed by modelling and simulation* - *provide a roadmap for the development and application of modelling and simulation, gaming and further adequate methodologies and tools* **IRRIIS** - *Determine a sound set of public and private sector requirements based upon detailed scenario and data analysis.* **ESFORS** - *Bring together the European stakeholders for security and dependability Information and Communication Technologies (ICTs) to address the security and dependability requirements of emerging software service platforms* **MEDSI** - *Integration of Geographical Information Systems with DB, decision-support management and an auditory system to develop an advanced system that will be able to give support on decisions in a crisis* **VITA** - *(Analyse) threat of Critical Infrastructures in Europe by natural disasters, manmade disasters and technical incidents,* **CRUTIAL** - *Investigation of models and architectures that cope with the scenario of openness, heterogeneity and evolvability endured by electrical utilities infrastructures;* - *Analysis of critical scenarios in which faults in the information infrastructure provoke serious impacts on the controlled electric power infrastructure;* - *Investigation of distributed architectures enabling dependable control and management of the power grid.*
Mid Term (3-8 yrs): *Components and architectures*	

Flexible architectures needed to mitigate cascading effects among ICT infrastructures and power systems	**CRUTIAL** - *Investigation of distributed architectures enabling dependable control and management of the power grid.* **IRRIIS** - *Develop MIT (Middleware Improved Technology), a collection of software components, which facilitates IT-based communication between different infrastructures and different infrastructure providers* - *Build SimCIP (Simulation for Critical Infrastructure Protection), a simulation environment for controlled experimentation with a special focus on CIs interdependencies*
Identification of transition steps toward more robust systems	
Assurance of the power infrastructure: security policies (procedures, protection, etc.) in the context of defence plans, communication of security risk, assurance cases	**RETE21** – *development and operation of the Power Grid for the 21st Century*
Long Term (8-15 yrs):	***protective measures, remedial actions and real time applications***
Real time applications for supervision & control encompassing EMS & ICT functions **Strategies for decentralized intelligence** **Self reconfiguring architectures and protection mechanisms**	
Implementation, testing and performance evaluation of the introduced and incremental new control concepts	

Table 4 – Project positioning against GRID objectives in the Awareness and Governance of Risk in Socioety area

Awareness and Governance of Risk in Society	
Near Term (0-3 yrs): Awareness Raising and Education	
Awareness raising campaign for business and policy decision makers and practitioners	**VITA** - *Increase the awareness and a sense of urgency on the need for CIP capabilities* **ESFORS** - *Bring together the European stakeholders for security and dependability Information and Communication Technologies (ICTs) to address the security and dependability requirements of emerging software service platforms* **DDSI** - *Establishing networks of interest among the leading European and international stakeholders (European institutions, national governments, industry and civil society)* - *Providing baseline data about dependability initiatives around the world* - *Preparing policy roadmaps targeted at industry, national governments and European institutions* **GridWise™ Alliance** - *It is a consortium of public and private stakeholders who are aligned around a shared vision. A vision of an electric system that integrates the infrastructure, processes, devices, information and market structure so that energy can be generated, distributed, and consumed more efficiently and cost effectively; thereby achieving a more resilient, secure and reliable energy system.*
Establish training curricula, programs and tools for risk assessment including professional education	
Proposal of security risk governance arrangement for the European power infrastructure	
Mid Term (3-8 yrs): Actions on Society and Organisations	
EU training programme for Power Engineers on security risk	

Consensus on Security Risk management & governance structures	
First set of EU security laboratories	**TRUST**: - Analysis, design and deployment of trusted systems. TRUST's Research programme encompasses: - Security technology - System science - Social science - Testbeds **TCIP** - Research plan is focused on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, and/or power emergencies.
Acceptance of standards for secure data exchange & communication	**IEC TC 57 & 65** - *Standardisation efforts in the process control and the power sectors*
Long Term (8-15 years): ***Deploy EU-wide security programme***	
EU wide training facilities for power engineers	

3 CONCLUSIONS

Among those considered in this review, the US-Canada Road Map is the closer in scope to the GRID one. However there are important differences between the two Road Maps – chiefly related to sponsorship and aim. These points basically explain the other differences related to participants, scope and timeframe. While the USCR is *directly sponsored by the US and Canada governments* in a joint effort, GRID is *partly funded by the Commission* through the EU framework. The USCR is *a collaborative work between industry and government* with active involvement and leadership of energy asset owners and operators, while GRID is lead by its research partners, and *performs consultation actions toward the industry* - stakeholders are directly involved in an advisory role only. The USCR is aimed at improving cyber security through a *coherent plan to be used by industry and government as a template for action*, while GRID is aimed at improving cyber security through a *research roadmap which by its nature may impact on cyber security in an indirect way and in a longer term*. By consequence, the USCR covers the whole energy sector and includes activities of testing, best practices, training and education, policies, standards and protocols, information sharing in addition to R&D, while GRID covers the electricity domain only, and mostly focuses on R&D in longer term timescales.

Concerning CI2RCO, its findings and recommendations are a valuable background for GRID and many of the general results of CI2RCO can be supported from the in-depth experience in the closer GRID sector, but in practice there is little overlapping. The same can be predicated for most of the generic EU projects quoted in Tables 3, 4 and 5, while power sector specific projects, like CRUTIAL, IRRIIS and VITA may contribute insight in the requirements analysis phase and specific solutions for control architectures and tools.

The other important EU Road Mapping efforts in the power sector partly funded in the EU framework, SmartGrids, RELIANCE and ERMInE, have a similar constituency (they are all Coordination Actions among stakeholders) but a far broader scope than GRID:

- SmartGrids is aimed at providing a Road Map for R&D concerning (mostly) electricity distribution and in longer term horizon (2030) than GRID. Several research themes may be concerned by the GRID Road Map;
- RELIANCE provides coordination on R&D among TSOs. It also focuses on improved cyber security, but did not elaborate a specific Road Map on this theme.
- ERMInE aims at collecting data about the present situation of electricity RTD in Europe and a Roadmap – defined as the potential evolution of the electricity sector in Europe.

Over time, a working relationship has been established with the three actions above, hence the GRID Road Map is expected to be taken as an input by those actions, and influence their outcome in the relevant areas.

Concerning the GRID Roadmap's objectives presented in chapter 5, it is apparent that, while a good number of the censed projects address short-term objectives considered by GRID, most medium term objectives are not addressed. Among them it is especially worth noticing:

- *Assessment of defensive strategies and incident reporting* (Risk Assessment)
- *Identification of transition steps toward more robust systems* (Control Architectures & Technologies)

Finally, it is worth noticing that most short- and medium-term objectives considered within the area Awareness and Governance of Risk in Society are not addressed at all – unless by US projects, namely:

- *Establish training curricula, programs and tools for risk assessment including professional education*
- *(proposal of) security risk governance arrangement for the European power infrastructure*
- *First set of EU security laboratories*
- *Acceptance of standards for secure data exchange & communication*

Hence focus of security relevant research concerning power systems need to be moved towards the above objectives.

REFERENCES

[1] Critical Infrastructure Protection: Challenges and Efforts to secure Control Systems. GAO-04-354, United States General Accounting Office. March 2004 http://www.gao.gov/

[2] International CIIP Handbook 2006 Vol. I. An inventory of 20 National and 6 International Critical Information Infrastructure protection policies. Myriam Dunn and Isabelle Wigert. ETH – Swiss Federal Institute of Technology Zurich.

[3] The European Union and cybercrime: insights from comparative federalism. Fernadno Mendez. Journal of European Public Policy. 506-527; Volume 12, Number 3 / June 2005

[4] Critical Infrastructures at Risk: Securing electric power supply. Wolfgang Kroger. International Journal of Critical Infrastructure 2006 – Vol.2, No.2/3 pp. 273-293

[5] Power system control and associated communications – Data and communication security. Technical Report IEC/TR62210 62210:2003 (E) 2003-05

[6] Draft Standard for Substation IED Cyber Security Standards, IEEE P1686 ™/D1 Prepared by the C1 Application of Computer-Based Systems Working Group of the Substation Committee. ECEEE 2006

[7] Description of the programme: 86 Energy Information Security (EIS), Electric Power Research Institute (EPRI), 2007 Portfolio http://mydocs.epri.com/docs/Portfolio/PDF/2007_P086.pdf

[8] OECD Futures Project on Emerging Systemic Risks, 2003 http://www.oecd.org/dataoecd/23/56/19134071.pdf

[9] Infrastructure to 2030: Telecom, Land Transport, Water and Electricity. OECD, International Futures Programme. ISBN: 9264023984

[10] Department of Homeland Security's Information Analysis and Infrastructure Protection. National Infrastructure Simulation & Analysis Centre. Fact sheet. http://www.sandia.gov/mission/homeland/factsheets/nisac/nisac_program_factsheet.pdf

[11] Sandia National Labs' Security Risk Assessment Methodologies. (Presentation) http://www.sandia.gov/ram/RAM%20Overview%20%20Presentation%20Aug%2006.pdf

[12] Arnold B. Baker et al. "A Scalable Systems Approach for Critical Infrastructure Security", SAND Report SAND2002-0877. Unlimited Release. Printed April 2002

[13] Cyber-Threats and Countermeasures: Towards an analytical framework for explaining threat politics in the information age. Myriam Dunn

[14] Gheorghe A.V., Masera M et al. "Critical Infrastructures at Risk: Securing the European Electric Power System", Springer, 2006 ISBN: 1402043066

[15] Cleveland, F "IEC TC57 Security Standards for the Power System's Information Infrastructure: Beyond Simple Encryption" Proceedings of PES TD 2005/2006 May 21-24, 2006 Page(s):1079 – 1087.

[16] Fridheim, H., Hagen J, Henriksen, S., "En Sårbar Krafforsyning - Sluttrapport etter BAS-3" FFI/RAPPORT-2001/02381, Norwegian Defence Research Establishment 2001 http://www.nve.no/FileArchive/97/Sluttrapport.pdf

[17] Dondossola, G., Lamquet, O., Torkilseng, A. "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems" CIGRÉ 2006 session. Paris, France. 27 August-01 September 2006

[18] Doorman, G., Kjølle, G., Huse, E.S., Flatabø N. "Vulnerability of the Nordic Power System, Main Report. Report to the Nordic Council of Ministers", Technical Report TR A5962, SINTEF Energy Research, ISBN: 82-594-2652-8, May 2004. Trondheim http://www.norden.org/energi/uk/06-3Final_Report4.pdf

[19] Doorman, G., Kjølle, G., Huse, E.S., Flatabø N. "Vulnerability of the Nordic Power System, Executive Summary. Report to the Nordic Council of Ministers", Technical Report TR A5968, SINTEF Energy Research, ISBN: 82-594-2658-7, May 2004. Trondheim http://www.norden.org/energi/uk/06-2Executive_Summary5.pdf

[20] Morch. A. Z., *Critical Infrastructure Protection (CIP): Overview over international expertise and R&D projects,* GRID Deliverable D7/CIP, September 2007.

[21] Stefanini, A. Masera M., Ciapessoni, E. *A Survey On Existing SCADA Security Standards,* Convegno ANIPLA 2006, Univ. di Roma La Sapienza, September 2006.

European Commission

EUR 23268 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Current efforts concerning ICT security of the power grid
Author(s):
Alberto Stefanini, JRC – IPSC
Andrei Z. Morch, SINTEF Energy Research
Giovanna Dondossola, CESIRicerca
Geert Deconinck, Katholieke Universiteit Leuven
Paul Friessem, Fraunhofer-SIT
Luxembourg: Office for Official Publications of the European Communities
2008 – 32 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593

Abstract

GRID is a Coordination Action funded under the Trust and Security objective of the IST Programme of the 6th Framework to achieve consensus at the European level on the key issues involved by power systems vulnerabilities, in view of the challenges driven by the transformation of the European power infrastructure and ICT integration. GRID wants to assess the needs of the EU power sector on these issues, so as to establish a Roadmap for collaborative research in this area.

The present report provides a survey on current efforts somewhat related to the objectives of GRID. Similar to GRID, a number of European and US endeavours have attempted in recent years to draw a Road Map so as to coordinate efforts concerning energy transport/distribution research and CIP.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

Publications Office
Publications.eu.int