



**European Cooperation
in the field of Scientific
and Technical Research
- COST -**

Secretariat

Brussels, 11 December 2008

COST 263/08

MEMORANDUM OF UNDERSTANDING

Subject : Memorandum of Understanding for the implementation of a European Concerted Research Action designated as Cost Action IC0806: Intelligent monitoring, control and security of critical infrastructure systems (IntelliCIS)

Delegations will find attached the Memorandum of Understanding for COST Action IC0806 as approved by the COST Committee of Senior Officials (CSO) at its 172nd meeting on 24-25 November 2008.

MEMORANDUM OF UNDERSTANDING

For the implementation of a European Concerted Research Action designated as

COST Action IC0806

INTELLIGENT MONITORING, CONTROL AND SECURITY OF CRITICAL INFRASTRUCTURE SYSTEMS (INTELLICIS)

The Parties to this Memorandum of Understanding, declaring their common intention to participate in the concerted Action referred to above and described in the technical Annex to the Memorandum, have reached the following understanding:

1. The Action will be carried out in accordance with the provisions of document COST 270/07 “Rules and Procedures for Implementing COST Actions”, or in any new document amending or replacing it, the contents of which the Parties are fully aware of.
2. The main objective of the Action is to develop innovative intelligent monitoring, control and safety methodologies for critical infrastructure systems, such as electric power systems, telecommunication networks, and water systems.
3. The economic dimension of the activities carried out under the Action has been estimated, on the basis of information available during the planning of the Action, at EUR 88 million in 2008 prices.
4. The Memorandum of Understanding will take effect on being accepted by at least five Parties.
5. The Memorandum of Understanding will remain in force for a period of 4 years, calculated from the date of the first meeting of the Management Committee, unless the duration of the Action is modified according to the provisions of Chapter V of the document referred to in Point 1 above.

A. ABSTRACT AND KEYWORDS

Everyday life relies heavily on the reliable operation and intelligent management of large-scale critical infrastructures, such as electric power systems, telecommunication networks, and water distribution networks. The design, monitoring, control and security of such systems are becoming increasingly challenging as their size, complexity and interactions are steadily growing. Moreover, these critical infrastructures are susceptible to natural disasters, frequent failures, as well as malicious attacks. There is an urgent need to develop a common system-theoretic framework for modelling the behaviour of critical infrastructure systems and for designing algorithms for intelligent monitoring, control and security of such systems. This COST Action (IntelliCIS) will contribute to the advancement of knowledge in the areas of computational intelligence and autonomous agents, with specific emphasis on the application of these methodologies in monitoring and controlling large-scale distributed complex systems. This will be achieved by the development of innovative techniques and algorithms for fault tolerant operation of critical infrastructures and their evaluation by theoretical analysis and simulation. The Action will be a catalyst for instigating interdisciplinary interaction and will promote collaboration between industry, academia and research organizations on the subject of security, quality, reliability, and efficiency of critical infrastructure systems.

Keywords: computational intelligence and system theory, critical infrastructure systems, electric power systems, telecommunication systems, water distribution networks.

B. BACKGROUND

B.1 General background

Modern societies have reached a point where everyday life relies heavily on the reliable operation and intelligent management of critical infrastructures, such as electric power systems, telecommunication networks, and water distribution networks. Designing, monitoring and controlling such systems is becoming increasingly more challenging as their size, complexity and

interactions are steadily growing. Furthermore, the performance objectives are expanding from the traditional goal of achieving smooth network operation to having high levels of security, accuracy, quality, efficiency, reliability, and fault tolerance. These critical infrastructures are susceptible to natural disasters, accidental failures, and malicious attacks. Besides emergency services, business critical services and private services can be disrupted for long and unacceptable durations when the operation of critical infrastructures is disrupted.

Intelligent management and control of critical infrastructure systems (CIS) is a timely and urgent research issue worldwide. The European Commission places a tremendous amount of emphasis on this topic as evident by the research themes (e.g., see the programmes on Information and Communication Technologies, Energy, Environment, Security) of the 7th Framework Programme. The issues addressed in this COST Action are highly relevant for Europe since this is the most densely populated region in the world, with a number of interconnected infrastructure networks that have different owners or operators. For example, the electricity grid is an interconnected network in most of the European countries with each sub network being managed and controlled by the respective Transmission System Operator. In November 2006, a local fault in Germany's power grid cascaded through large areas of Europe, resulting in 10 million people left in the dark in Germany, France, Austria, Italy, Belgium, and Spain.

The issue of secure, reliable, and optimal operation of critical infrastructure systems receives considerable attention worldwide and in particular in the United States. A number of consortia and research teams are actively working in this field with the support of the industry and the US government. For example, the Complex Interactive Networks/Systems Initiative (CIN/SI) is a joint program by the Electric Power Research Institute (EPRI) and the US Department of Defense that was formed to study the interdependency between critical infrastructure systems and to develop tools and techniques for handling failures or emergencies.

Critical infrastructure systems have many common characteristics and requirements, which naturally point to the need for a common methodological framework. They are large-scale, complex, spatially distributed and data-rich systems. Moreover, they are dynamic and their operation is subject to significant uncertainty. Last, but not least, it is critical in modern societies that the operation of these systems is uninterrupted despite any component failures. The objective of the IntelliCIS COST Action is to combine deep knowledge of the application domains with tools from computational intelligence, system theory and adaptive systems to develop smart monitoring and control solutions based on the principles of intelligent data interpretation and decision, self-aware/self-improve/self-healing design, scalability, flexibility, modularity and fault tolerance.

This COST Action will bring together researchers working in various different fields, in order to enable the cross-fertilization between research areas, knowledge transfer and technology transfer between areas and between Academia and Industry. One of the main advantages of this Action is that it will bring together scientific communities that share similar problems but are currently lacking of a common network in order to share ideas and solutions. The Action will help in coordinating the research efforts in Europe and will strengthen Europe's networking capacity in this critical field of research.

This Action fits better within the objectives of the COST framework, rather than other research funding programmes, such as FP7. IntelliCIS has a multidisciplinary nature, addressing key and critical aspects of energy infrastructures, communication infrastructures and water infrastructures, and their management, monitoring and control through innovative techniques based on the principles of distributed, multi-level control, intelligent agents, adaptivity, fault tolerance and self-healing approaches aided by intelligent sensors and actuators. No existing COST Actions address this multidisciplinary research area, and therefore this Action can lead to a concentrated effort in bringing together researchers working in these fields in Europe and help in strengthening the scientific and technical presence of Europe in decision-making, policy-making and development of new methods and tools. This COST Action will lead to the strengthening and cross-fertilization of research activities from areas that until now have had little evidence of working together. Therefore, COST is the ideal framework to help initiate and promote these activities.

B.2 Current state of knowledge

Critical infrastructures are large-scale, complex, interconnected, and distributed systems. Such systems are progressively becoming larger in scale and more complex, making their management more challenging. Due to technological advances and deregulation, critical infrastructures are becoming more heterogeneous and distributed, making it more difficult to secure reliable operation. Their interconnectedness makes critical infrastructures vulnerable to failures, which may be caused by natural disasters, material failures, human error or by intentional attacks. On the other hand, their interconnectedness also allows a level of operational redundancy for fault tolerance, provided it can be utilized effectively. As technology advances, the interactions in the reliable operation and management between different infrastructures are becoming increasingly more important. For example, there are strong links between the reliable operation of power grids and communication networks, as well as between power networks and water networks. Therefore, there is a crucial and urgent need to investigate under a common framework the reliable operation and interactions between critical infrastructures.

During the last few years there has been significant research on the modelling, monitoring and control of critical infrastructure systems. The vast majority of this work has been application specific. For example, in electric power systems there has been a lot of work on modelling, sensor and actuator instrumentation, simulation and prediction tools, etc. Intelligent electronic devices are starting to become available for monitoring and controlling electric power systems. These devices may include sensing capabilities for on-line measurement, actuators for controlling certain variables, microprocessors for processing information and making decisions based on designed algorithms, and telecommunication units for exchanging information with other electronic devices or possibly with human operators. Such devices, which are sometimes referred to as intelligent agents, provide fundamental tools for intelligent monitoring, control and safety of critical infrastructure systems.

Recent technological advances in computing hardware, sensors/actuators, communications and real-time software have provided the capability to generate huge amount of data in real time. This data, or information, is generated continuously every day in a wide range of infrastructure systems, as well as in other applications. The generated data is in various forms (for example, time series measurements, audio, video, etc) and quite possibly from different geographical locations. As the volume of data generated is rapidly increasing, one of the most important research challenges in the new technology is the development of information processing methodologies that can be used to extract meaning and knowledge out of the ever-increasing electronic information that becomes available. Even more important is the capability to utilize the data knowledge that is being produced such that one can design software and devices that operate autonomously and cooperatively in some intelligent manner. The ultimate objective is to design intelligent systems or intelligent agents that can make appropriate real-time decisions in the management of large-scale complex systems, such as critical infrastructure systems.

This COST Action aims at developing an innovative common framework for monitoring and control of different critical infrastructure systems based on the following concepts:

- Decentralized Monitoring and Control. As complexity in infrastructure systems increases, there is a need to develop a decentralized (instead of centralized) monitoring and control framework, where each node in the network is a potential location for a sensor/actuator/controller device, which is referred to as an intelligent agent.
- Intelligent Agents. An intelligent agent is located at a node of the network and is able to gather data, process data, make decisions, change a control variable, and communicate information to other agents. These agents may be in the form of hardware or in software. Some intelligent agents are specialized, in the sense that they may be doing a very specific task (such as sensing). A key objective for the intelligent agents is to cooperate with each other based on some global objective.
- Adaptive and Learning Capabilities. Since it is impossible to model exactly all the dynamics of a complex infrastructure system, it is important to devise methods for adaptation and learning of the intelligent agents. These methods will be based on neural network techniques and adaptive control.

- Fault Accommodation and Self-Healing. Using techniques from fault diagnosis and health monitoring, the objective is to develop algorithms that are able to predict or determine a failure as soon as possible, isolate the location of the failure and reconfigure the nominal control algorithms to achieve fault recovery and self-healing.

- Intelligent Decision Support Systems. A very important parameter in monitoring and controlling critical infrastructure systems is the role of human operators. The objective is to design intelligent decision support systems using computational intelligence to enhance the decision making capabilities of operators (considering the overwhelming number of alarms that are typically received after a fault and the associated short response time required) and to assist them in normalizing the state of the system at all times. Intelligent decision support systems are capable of processing real-time sensor information to provide high-level information to human operators in a way that can be easily understood and visualized.

B.3 Reasons for the Action

Critical infrastructures are crucial to the social and economic well-being of people worldwide. This COST Action aims at contributing to the development of smart and reliable infrastructures through the use of dedicated intelligent system techniques. This requires collaboration between researchers from diverse communities working in computational intelligence, system theory, power systems, communications, and water systems. The COST framework provides an ideal avenue to bring together researchers from different communities in order to share as well as enhance their expertise through collaboration.

The Action is derived both from an economic/societal need as well as from a scientific/technological need to develop better approaches for handling such complex and safety critical systems. The societal and economic need arises due to the increasing demand for continuous and reliable supply of electric power, water and information at all times and at all places. The scientific motivation for the Action arises by the urgent need to develop a common framework for intelligent monitoring, control and safety of large-scale interconnected systems, with emphasis on specific critical infrastructure systems.

The general problem of management and security of critical infrastructures involves researchers working in the government, in large established companies (power and telecommunication companies), in Small/Medium Enterprises-SMEs (e.g., software companies for water systems), as well as in academia and in research centres. Since the background and objectives for the people involved may be quite different, a COST Action on this topic will help significantly in the rapid and efficient transfer of knowledge between industry, government and academia.

B.4 Complementarity with other research programmes

This COST Action is complementary to several European research projects (see Section E.3) dealing with management and security of critical infrastructure systems. However, the topics of existing research projects are focused on specific aspects of monitoring and control of large-scale systems or on specific applications. Typically, the research communities dealing with energy infrastructures work separately from the researchers working in communication networks, which in turn work independently from researchers working in water systems infrastructures.

This COST Action brings these research communities together, not only to allow cross fertilization of ideas but also to help develop a common framework for modelling, measurement, monitoring and control of large-scale, interconnected safety-critical systems. Moreover, it provides a way for investigating interactions and interdependencies between different infrastructures. The Action combines application domain expertise and knowledge with techniques, algorithms and analysis tools from system theory, computational intelligence and optimization. The already available knowledge obtained through national and EU-wide research projects will help in establishing IntelliCIS as a liaison for interaction between related activities in intelligent monitoring, control and safety of critical infrastructure systems.

C. OBJECTIVES AND BENEFITS

C.1 Main/primary objectives

The main objective of the Action is to develop innovative intelligent monitoring, control and safety methodologies for critical infrastructure systems, such as electric power systems, telecommunication networks, and water systems.

C.2 Secondary objectives

The main secondary objectives of the Action are:

1. To develop innovative intelligent management, monitoring and control models and algorithms for fault tolerant operation of Critical Infrastructure Systems (CIS).
2. To develop behavioural and functional models for accurately characterizing the operation of CIS under steady state, dynamic, and post-fault conditions.
3. To develop interactive models between more than one CIS; for example, modelling the interdependence between communication and electric power networks.
4. To develop network design and recovery techniques which can give solutions for a more efficient network that can mitigate massive attack or catastrophic failure scenarios.
5. To design inter-infrastructure fault management scenarios (including fault detection, isolation and recovery).
6. To develop a theoretical framework that enables the analysis of the robustness of large-scale, complex and distributed systems.
7. To refine and apply tools and methodologies from computational intelligence and system theory for the management, monitoring, and control of electric power systems.

8. To develop network security models to enhance network security, and to develop resource allocation and Quality of Service (QoS) provisioning methodologies for telecommunication networks.
9. To investigate Wireless Sensor Network (WSN) based technologies as effective solutions for the problem of distributed, reliable and economic monitoring of CIS.
10. To develop optimal sensor and actuator placement methodologies for control, health monitoring and security of water distribution systems.
11. To contribute to the training of early-stage researchers and the establishment of a network of young researchers on the topics covered by IntelliCIS.
12. To stimulate and promote collaborative research by structuring and developing concept reports for future research proposals on the national and European level.
13. To establish a link with industrial partners and promote academic and industrial collaboration, eventually resulting in commercial applications.
14. To identify grand challenges in monitoring, control and security of CIS.
15. To investigate similarities and connections with other critical infrastructure systems (for example transportation systems and gas and oil networks).

The following quantitative indicators will be used to evaluate these specific objectives:

1. Number of researchers, groups and companies participating actively in the Action activities
2. Number of joint papers in journals and conference proceedings

3. Number of transnational collaborative research proposals prepared
4. Number of training activities and number of people trained
5. Number of researcher exchanges and scientific missions supported by the Action
6. Number of software and hardware tools developed
7. Number of scientific achievements generated in this COST Action.

The suggested quantitative evaluation criteria are listed in Section C.3.

C.3 How will the objectives be achieved?

The above objectives will be achieved through a close collaboration between the researchers involved in this Action coming from various different fields, enabling cross-fertilization between research areas, knowledge transfer and technology transfer between areas and between Academia and Industry. An important way to achieve the Action's objectives is by research exchange visits between different organizations. In these Short-Term Scientific Missions new valuable knowledge is gathered with regards to the theory and the applications of the methods and tools investigated, and the foundations for future collaborations are set. The expertise and knowledge of leading European experts in the scientific fields of the Action will be infused through networking to other Action participants. The exchange of the latest scientific results both from academia, industry and research organizations will be instrumental in achieving the Action's objectives.

The means to achieve these objectives are summarized below, providing some quantitative targets:

1. Networking will reach at least 65 institutions in 25 countries (51 institutions in 21 countries have already shown interest for this Action)
2. Networking will be extended to at least 25 companies (7 companies, both SME and large corporations have already expressed their interest for this Action)

3. About 10 collaborative, transnational projects on related topics will be submitted to national and European level programs
4. Management Committee meetings will take place up to 3 times a year to facilitate better and more intense communication among members
5. A project website listing upcoming and past activities, paper abstracts and presentations will be prepared by the Action participants
6. Two workshops (one every two years)
7. Two training schools (one every two years in alternate years with the workshops)
8. Three meetings per year
9. Over 100 publications in international peer reviewed journals and conference proceedings as a result of the scientific projects and yearly conferences of the Action
10. Some 20 scientific achievements as a result of the collaborative work within the Action
11. 20 Short-Term Scientific Missions and research exchanges within the Action
12. Annual progress reports by each Working Group
13. A final report describing the project outcomes and successes
14. Organization of at least 4 special sessions at international conferences.

C.4 Benefits of the Action

The Action has both technological and societal benefits. It supports cutting edge basic research in the fields of monitoring, control and safety through collaborative work and provides a practical viewpoint due to the participation of the industry. The main benefit is the exchange of expertise and knowledge, the development of a scientific community that may be active in promoting other actions at the European level, and the training of young scientists with a multi-disciplinary curriculum. The networking dimension of the Action will have immediate benefits in preventing unnecessary duplication of research work between different groups. It will coordinate the existing efforts and set goals and directions for future work. In this way it will help the community to optimally distribute research tasks, time and person-power.

In particular, the benefits of the Action are:

- Creates the critical mass for a strong interdisciplinary research team that can tackle challenging engineering problems related to the monitoring, control and security of CIS
- Promotes the technology transfer from academia to the industry and other government organizations
- Promotes knowledge transfer between organizations and researchers, as well as between research areas through cross-fertilization of ideas
- Facilitates the collaboration between researchers with diverse backgrounds and expertise to create synergies
- Provides the opportunity to initiate conferences/symposia on intelligent management of CIS
- Creates solutions to a wide range of real life problems that have a direct effect to the safety, well-being and prosperity of society
- Ensures that the consortium partners (including participating SMEs) have a high level of up-to-date expertise of the latest science and technology developments in the areas of the Action
- Diminishes the economic and knowledge discrepancies between the Western and Eastern European countries (if possible all COST countries will be targeted for partnership in this Action)
- Develops tools for the better management, monitoring and control of electric power systems to avoid blackouts and to improve power quality and service

- Develops network security models in order to enhance network security, and develops resource allocation and Quality of Service provisioning methodologies for telecommunication networks
- Develops optimal sensor and actuator placement methodologies for control, quality monitoring and security of water distribution systems.

This COST Action will be an effective way to close the gap between European industry and academia, and the technology gap between the USA and Europe, by making faster and more efficient the use of the scientific know-how in Europe through increased networking at the top level. Critical infrastructure systems are of crucial importance to the European well-being and economy, as well as an enormous scientific and commercial growth potential. An Action on these topics is therefore a timely and much-needed contribution to Europe in order to assist in the increase of security of CIS, as well as to the development of novel technological tools, methodologies and processes that can allow Europe to gain a technological edge over the USA which is also investing heavily in these areas.

C.5 Target groups/end users

There are two main target groups in this Action:

- (a) Researchers in academia and research organizations

Research in the monitoring, control and security of critical infrastructure systems is a vital and crucial scientific area. A large number of European researchers are working in this area and are expected to participate in the Action activities through their Universities and research laboratories/organizations. Basic research work in the fields of the Action can be generalized in other related research areas, thus targeting a wider scientific audience.

(b) Researchers in industry and government organizations

Critical infrastructure systems attract the attention of a multitude of industries, government organizations, SMEs, start-ups and spin-off companies. They will be the end users of the generated knowledge, the research results and the regulatory or scientific methodologies developed by the Action researchers through the collaborative activity. These partners will be invited to the meetings of the Action.

D. SCIENTIFIC PROGRAMME

D.1 Scientific focus

Many large-scale critical infrastructure systems, even though seemingly very different, may share significant common aspects that can be exploited for the development of a common framework. Such a framework will create synergies from the cross-fertilization of ideas between the different areas and will lead to the development of better management policies that will facilitate more reliable and robust operation of critical infrastructure systems. Some of the common characteristics of the large-scale critical infrastructure systems that will be investigated include:

- They are dynamic and very complex
- Their behaviour changes over time (no stationarity), thus they require adaptive strategies
- They are physically distributed and, typically, there is no single central controller that oversees the safe operation of the entire system
- They are data rich; there are many sensors that collect huge amounts of data
- They have high uncertainty

This Action will adopt a methodology based on the intelligent systems approach that utilizes tools from system theory, computational intelligence, optimization, networks and graph theory, fault diagnosis, as well as simulation and hardware tools. The objective is to combine deep knowledge of the application domain with tools from the intelligent system approach to develop smart monitoring and control solutions based on the principles of intelligent data interpretation and decision, self-aware/self-improve design, scalability, flexibility, modularity and fault tolerance. The COST Action is flexible enough to incorporate a wide array of projects varying from fundamental research on computational intelligence and networked control applied to the critical infrastructure systems under investigation, to specific applications and problems facing these infrastructure systems.

On an abstract level, Critical Infrastructure Systems (CIS) consist of nodes interconnected together with links (arcs) that enable the flow of certain variables from one node to its neighbours. For example, in water systems, the links are the pipes and the flows consist of transport of water while in communication networks there are communication links that are used to transport packets or (more generally) information. Furthermore, each infrastructure has a number of Intelligent Agents (hardware and/or software) that are appropriately located in the underlying network (relevant infrastructure) that have sensing capabilities to collect data, have computational capabilities to process the data and make decisions, have communication capabilities to send/receive information to/from other agents and have actuators to take control actions (autonomously or with human intervention). A key research task of the IntelliCIS COST Action is to investigate the interaction between the Intelligent Agents, both from a theoretical perspective as well as from an application perspective (i.e., as they are used in different critical infrastructure systems).

The Intelligent Agent behaviour and their interactions create research challenges that will be investigated during this COST Action.

- Decentralized Monitoring and Control. An action of one agent may have both a local and a global effect which are not always fully understood. This issue becomes more and more difficult as infrastructures grow larger and larger and include a large number of agents.
- Agent Collaboration. In order to achieve the global objectives set for each infrastructure, it is inevitable that the intelligent agents need to collaborate between themselves. How this collaboration should take place is an important question that will be addressed by the Action.
- Heterogeneous Agent Collaboration. How should agents on different infrastructure networks interact with each other in order to achieve certain objectives.
- Adaptive and Learning capabilities. The underlying networks evolve over time thus the agents should be adaptive and have learning capabilities to appropriately change their behaviour. Furthermore, such quality is needed in order to address possible modelling inaccuracies.
- Fault Accommodation and Self-Healing. The underlying infrastructure generally consists of unreliable components that can fail due to usage or due to a deliberate attack. The agents should be able to predict or determine a failure as soon as possible, isolate the location of the failure and reconfigure the distributed control algorithm to achieve fault accommodation and self-healing.

- Intelligent Decision Support Systems. A very important parameter in monitoring and controlling critical infrastructure systems is the role of human operators. The objective is to design intelligent decision support systems using computational intelligence to enhance the decision making capabilities of operators (considering the overwhelming number of alarms that are typically received after a fault and the associated short response time required) and to assist them in normalizing the state of the system at all times. Intelligent decision support systems are capable of processing real-time sensor information to provide high-level information to human operators in a way that can be easily understood and visualized.
- Architectural Issues: One of the key issues that require attention is the determination of the overall architecture that connects the local intelligent agents. One of the approaches that can be considered is the hierarchical architecture, where the information from a number of local controllers is coordinated by regional or global controllers.

Wireless Sensor Network (WSN) Technology is an effective technology that can be used to address many of the problems of decentralized and distributed monitoring and control of CIS. This technology will be investigated during this Action for various infrastructures. Furthermore, some more fundamental questions will be addressed such as data collection and storage, processing, aggregation, and information fusion.

D.2 Scientific work plan – methods and means

The activities of this Action will be organized in four Working Groups (WG). Three WGs will promote research specifically dealing with intelligent monitoring and control of specific application infrastructures. In addition there will be a WG which will focus on the development of a common methodological framework for bringing together the various application domains. This will lead to the cross-fertilization of ideas between the areas and will assist in achieving one of the fundamental objectives of this Action which is to bring together researchers from different research fields with common problems. An additional objective is to investigate models and design methodologies for the interaction and interdependence between application infrastructures; for example, the interaction in monitoring communication networks and electric power networks.

The Working Group themes are chosen so as to allow inclusion of new members to join at a later stage, or members to join more than one Working Group. The objectives of the four Working Groups are:

WG 1: Intelligent systems approaches for critical infrastructure systems (CIS)

- Make contributions to the theory of control of large-scale CIS.
- Develop a theoretical framework that will enable the analysis of the robustness of large-scale complex and distributed systems.
- Develop models that can capture the dynamical behaviour of large-scale CIS.
- Develop computational intelligence tools for monitoring CIS.
- Investigate and develop fault models that are appropriate for CIS.
- Investigate and develop inference and data mining tools for CIS.
- Design of methodologies for intelligent management, monitoring and control of CIS
- Develop algorithms and tools (hardware/software) for CIS.
- Classification of common problems and solutions for each of the research areas of the Action.
- Develop methodologies for monitoring, control and safety of more than one infrastructure in a common framework.

WG 2: Reliable management and control of electric power systems

- Investigate various mechanisms for cascade network collapse.
- Design of methodologies for intelligent management, monitoring and control of electric power systems
- Design alarm processing techniques and tools for on-line monitoring, having the capability of taking (limited) automatic corrective actions.
- Refine and apply tools and methodologies from computational intelligence
- Investigate wireless sensor network based solutions for monitoring and control of power networks.
- Investigate similarities and connections with other energy systems.

WG 3: Reliable management and control of telecommunication networks

- Investigate security models as they apply to various networks (e.g., wireless, optical).
- Design of methodologies for intelligent management, monitoring and control of communication systems.
- Develop network security models and use them to enhance network security.
- Develop resource allocation and Quality of Service provisioning methodologies.
- Investigate similarities and connections with transportation systems.

WG 4: Health monitoring and control of water systems

- Design of methodologies for intelligent management, control and health monitoring of water distribution systems.
- Security of water distribution systems and early detection systems.
- Investigate wireless sensor network based solutions for monitoring and control of water systems.
- Optimal sensor and actuator placement for control, health monitoring and security of water systems.
- Development of control-oriented models of dynamics in drinking water distribution networks.

The COST Action will facilitate the coordination and concentration of the efforts of the individual participating entities, as well as it will initiate a number of additional research projects which will be carried out by the participants. The projects will be arranged in such a way that they will enable interdisciplinarity and maximum interaction between the Working Groups.

E. ORGANISATION

E.1 Coordination and organisation

The COST Action will be coordinated by a Management Committee (MC). The Chair and the Vice-Chair of the MC will be elected at the kick-off meeting to be held at the start of the Action. Each party will have two representatives in the MC. In addition, Chairs and vice-Chairs for the Working Groups, a web site Coordinator and Transfer of Knowledge Coordinator will be appointed at the kick-off meeting. A Secretariat for the MC will also be appointed who will be supporting the Chair with administrative matters.

Following the kick-off meeting, MC meetings will take place up to three times a year. These meetings will deal with all strategic issues concerning the Action such as the approval of new Working Groups, the termination of existing Working Groups, organization of workshops, approval of Short-Term Scientific Missions (STSMs), ways to improve communication between the Action participants, ways to improve dissemination of the results of the Action, etc. The MC will also be in charge of coordinating the editorial production of the Annual Reports of each WG, which are due at the end of each year that the Action is running. For each WG the first Annual Report will contain an extensive state-of-art review, the next two Annual Reports will contain the progress of the Action, and the last Annual Report will contain the conclusions of the Action. The MC will decide on urgent matters by electronic communication (e-mail).

The research associated with the Action will be coordinated by the Working Groups (WG), through their Chairs and Vice-Chairs. In order to promote collaboration among the researchers (and thus fulfilling the overall objective of the Action), the partners will also be encouraged to additionally form Focus Areas (FA) targeting specific applications and research problems within or across WGs. Furthermore, FAs allow additional flexibility to the Action, in order to accommodate new members and new applications. To encourage participation and initiatives of early-stage researchers, the Vice-Chair of each WG will be an early stage-researcher.

Two workshops (one every other year) will be organized in parallel with the MC meeting. The workshop will be open to the entire scientific community and can potentially be held jointly with some other conferences. The goal of the workshop would be to summarize the current status and future trends of the research field. It will include all aspects of critical infrastructures relevant to this Action: intelligent systems, power grid networks, telecommunication networks, and water distribution networks. Participants and invited speakers from European and non-European countries, such as Japan and the USA, will update the members of the COST Action on the most recent results, as well as on general trends within the global critical infrastructure research community.

Short-Term Scientific Missions (STSMs) for exchange of students, as well as senior scientists, between the participating research groups will be promoted by the MC. Young researchers and women scientists in particular will be encouraged to participate in such exchanges. A website for the Action will also be set up at the start of the Action. This website will assist in the exploitation and dissemination of the results of the Action, both externally and internally. Through this website, the partners will be provided with access to the various technical reports, related projects, STSMs, etc. The WG Chairs will be responsible for maintaining the website.

E.2 Working Groups

The activities of this Action will concentrate on four main research areas, three of which promote research dealing with intelligent monitoring and control of specific application infrastructures, while the remaining research area develops a common methodological framework for bringing together the various application domains. This will lead to the cross-fertilization of ideas between the areas and will assist in achieving one of the fundamental objectives of this Action, which is to bring together researchers from different research fields with common problems. The area themes are chosen so as to allow inclusion of new members to join at a later stage, or members to join more than one theme.

Based on these research areas, this Action will establish four Working Groups (WGs) that will be responsible to complete all the scientific goals set forth by this Action. Working Group Chairs will be elected and their responsibility would be to coordinate the activities of the Working Groups, lead the scientific discussions, and provide the Management Committee with an annual report on the progress of the Working Group. A WG Vice-Chair will also be elected. All researchers participating in this Action will be invited to join one or more Working Groups, depending on their research interests and activities. In the course of the Action, new Working Groups can also be established depending on the needs of the Action. The contents of the four Working Groups are:

- WG 1: Intelligent systems approaches for critical infrastructure systems (CIS)
- WG 2: Reliable management and control of electric power systems
- WG 3: Reliable management and control of telecommunication networks
- WG 4: Health monitoring and control of water systems

E.3 Liaison and interaction with other research programmes

This Action will establish liaisons with other COST Actions (e.g., COST 291 (Towards digital optical networks), COST 295 (DYNAMO Dynamic Communications Networks: Foundations and Algorithms), COST 2100 (Pervasive Mobile & Ambient Wireless Communications), etc) as well as other FP7 European research projects (e.g., DIESIS (Design of an interoperable European federated simulation network for critical infrastructures), WIDE (Decentralized and Wireless Control of Large-Scale Systems), VIKING (Vital Infrastructure, Networks, Information and Control Systems Management), MOBESENS (Mobile water quality sensor system), COOLNESS (Cooperative transmission and cross-layer techniques for secure wireless sensor networks), PRODI (Power plants robustification based on fault detection and isolation algorithms), REACCESS (Risk of energy availability: common corridors for Europe supply security), etc).

Interactions with other COST Actions and FP7 European research projects can be established by joint meetings, for example as part of a commonly organized Conference. The outcome of such interactions will be joint publications as well as product development between partners of this Action and researchers external to the Action.

E.4 Gender balance and involvement of early-stage researchers

This COST Action will respect an appropriate gender balance in all its activities and the Management Committee will place this as a standard item on all its MC agendas. The Action will also be committed to considerably involve early stage researchers. This item will also be placed as standard item on all MC agendas. To promote gender diversity and balance of the researchers involved in this Action, the Management Committee will be responsible for building and maintaining diversity in all teams by nationality and race. Furthermore, every effort will be made to maintain a good gender balance in the elected leaders of this Action (Chair, Vice-Chair, MC members, WG leaders) who cover coordinational, organizational and other related responsibilities. In addition, early stage researchers are also invited to participate in MC meetings.

To promote gender diversity this Action will promote enhanced involvement and visibility of distinguished women senior researchers in co-advising and cross-training exchanges, seminars, tutorials and conferences. Similarly, women team members and postgraduate students in this Action will be specifically supported to participate in exchange visits abroad, conference presentations of their work, leading and peer-mentoring of undergraduates in team projects etc, to provide live examples of success in postgraduate education.

This Action will also encourage the participation of early stage researchers (MS, PhD students and young postdoctoral scientists) and in particular, young scholars in the research projects that will be carried out within the WGs. Four of the initiators of this Action are young scholars, including one female young scholar. Moreover, each WG will have a Vice-Chair, who will be an early-stage researcher. Finally, the Action will encourage and promote Short-Term Scientific Missions for young researchers on a competitive basis.

F. TIMETABLE

The Action will have a total duration of four years. Every year there will be three Management Committee (MC) Meetings. Furthermore there will be two Workshops and two Ph.D. Student Training Schools as shown in the following table.

| Month | Year 1 | Year 2 | Year 3 | Year 4 |
|-------|---------------------------------------|-------------------------------|------------------------|-------------------------------|
| 1-4 | Kick-off Meeting Website Operative | MC Meeting | MC Meeting | MC Meeting |
| 5-8 | Workshop MC Meeting | Training School MC Meeting | Workshop MC Meeting | Training School MC Meeting |
| 9-12 | MC Meeting | MC Meeting | MC Meeting | MC Meeting |

The Action will start with the kick-off meeting where the Working Group (WG) leaders will be elected. Furthermore, within the first 3 months of the Action, the Action website will become operative.

The Action will organize four three-day events (two workshops and two training schools). During these events a half-day Management Committee meeting will also take place. The remaining MC meetings will be two-day events where half day will be devoted to the MC meeting and the remaining time will involve technical meetings typically organized by the Working Groups (WG). During the Workshops, Training Schools and MC Meetings, renowned experts from Academia and Industry will be invited to give presentations. Additional technical meetings can be organized ad-hoc outside the MC meetings if necessary. Each MC meeting will take place in a different participating COST country in order to allocate organization responsibilities among each participating country and promote collaboration. Finally, it is expected that after the kick-off meeting and for the duration of the Action, there will be several Short-Term Scientific Missions (STSM) among the different research groups.

G. ECONOMIC DIMENSION

The following COST countries have actively participated in the preparation of the Action or otherwise indicated their interest: BE, CH, CY, CZ, DK, FI, FR, DE, GR, HU, IE, IL, IT, NL, NO, PL, RO, ES, SE, TR, UK. On the basis of national estimates, the economic dimension of the activities to be carried out under the Action has been estimated at 88 Million € for the total duration of the Action. This estimate is valid under the assumption that all the countries mentioned above but no other countries will participate in the Action. Any departure from this will change the total cost accordingly.

H. DISSEMINATION PLAN

H.1 Who?

The intended target audience for the dissemination of the Action results and findings is the following:

- The COST Action Members
- The international research community in the areas of critical infrastructure systems, intelligent systems, electric power systems, telecommunication networks, and water systems
- Other related research frameworks and bodies (such as CenSCIR CMUs Centre for Sensed Critical Infrastructure Research)
- Individual researchers (outside the Action) in the above areas
- International and regional industry in related fields (with a strong focus on SMEs)
- Policy makers and planners (such as CIP Critical Infrastructure Protection centres and government bodies in Europe and the USA)
- Standardization bodies, (such as the European Committee for Standardization and ITU-T (International Telecommunications Union))
- Professional bodies, such as the IEEE.
- Trade/professional magazines
- The general public

H.2 What?

The intended methods of dissemination are the following:

- Action website/database listing: upcoming and past activities, annual reports from the Action, paper abstracts and presentations prepared by the Action partners, technical information of developed tools (software and hardware), abstracts of joined research proposals initiated by the Action partners, Action progress reports (the website will include both public and private password protected sections for working and coordinating documents)

- Electronic discussion forum, hosted by the Action website, for interactive communication and support between the Action partners and other partners and individuals interested in the Actions activities (with a special focus on PhD-students, post-doctoral fellows and other young researchers)
- Three meetings of the Action partners per year, for internal dissemination
- Two biennial workshops, with public proceedings
- Two biennial training schools (in alternate years with the workshops)
- Publications: joint papers in international peer-reviewed journals and conference proceedings, technical reports
- Organization of special sessions at international conferences
- Dissemination of the results to the Industry will be mainly carried out via personal contacts of the Action partners as well as during international and regional conferences
- Contributions to standardization bodies and invitation to such bodies to participate in scheduled standardization meetings
- Distribution of the Action findings and recommendations to the general public.

H.3 How?

Dissemination methods are classified as internal and external. The internal dissemination activities target all Action members, in order to make all research results, findings, and recommendations available to them. The outline of the Action website will be presented and finalized at the kick-off meeting, so that it can be launched as early as possible. The website will act as an on-line database and communication and support tool (through the electronic forum) among the partners, allowing efficient and quick dissemination of research results. Website accesses and other related statistics will be collected and analyzed on an annual basis, so that the website's impact (in terms of format and content) can be evaluated and updated as needed during the course of the Action. Internal dissemination will also be enhanced through the scientific exchanges of researchers, the periodic scheduled meetings within the Action, and the biennial training schools which will target young researchers and the industry for science and technology transfer purposes.

External dissemination activities target audience outside the Action network and intend to make public the results of the research efforts related to the Action through participation in international conferences, joint publications in international peer-reviewed journals, organization of special sessions in the field of intelligent monitoring, control and security of critical infrastructure systems, and the creation of liaisons with other COST Actions. The Action website will also play an important role in the external dissemination activities. Dissemination to the general public will be achieved via popular science articles, seminars, and audio and television broadcasts. Finally, it is emphasized that the Action will participate in platforms and coordinating actions, and will focus on the Industry University collaboration by allowing the Industry Members to take on a consulting role especially towards young researchers and shape the research efforts.

Other dissemination efforts will focus towards the enlargement of the Actions by attracting and including additional important members from the European research community in the field of critical infrastructure systems, as well as smaller groups and upcoming young researchers from Europe. Besides the website which will include invitations to join the Action, recruitment of new collaborators and open research positions related to the Action activities will be announced in the academic press, at international and regional conferences, as well as other on-line services (such as the website ERACAREERS, the Pan-European Researchers Mobility Portal). Furthermore, specially appointed Action members will act as contact persons to the external scientific community for recruiting new researchers, supporting them in the integration of the Action's scientific results and tools in their research (with special focus on graduate students, post-doctoral fellows, and other young researchers), and for communication with industry representatives. These outreach activities will be collected and analyzed on an annual basis, and included in the yearly Action progress report.