August/September 2005, Volume 1, Number 2

ECN

European CIIP Newsletter

Co-ordinating the development of a Strategic Research Agenda

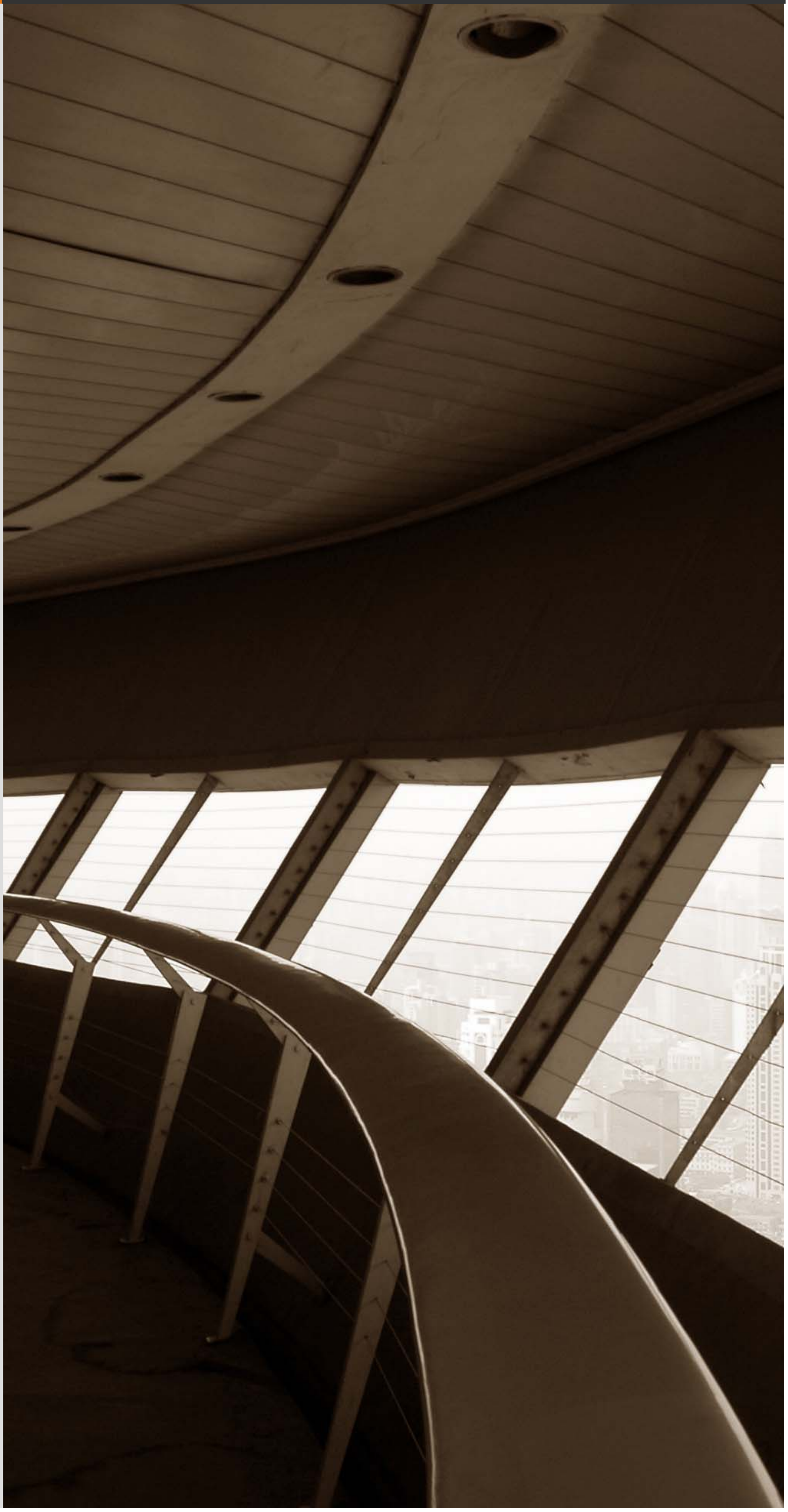
SAFEGUARD, a proposal to improve the survivability

The Critical Infrastructure Protection Program USA

First IEEE International Workshop on CIP

Special Interest Group KRITIS formed at German Informatics Society

CI²RCO



> About ECN
ECN is co-ordinated with
The European Commission, Dr. Andrea Servida
For 2005-2006, ECN is financed by the CI^{2}RCO project
The CI^{2}RCO project is an IST FP6 Co-ordination Action,
funded by the European Commission
under the contract no 015 818

>For ECN registration send any email to:
subscribe@ciip-newsletter.org

>Article can be submitted to be published to:
submit@ciip-newsletter.org

>Questions about articles to the editors can be sent to:
editor@ciip-newsletter.org

>General comments are directed to:
info@ciip-newsletter.org

>Download side for specific issues:
http://www.ci2rco.org/

The copyright stays with the editors and authors respectively, however
people are encourage to distribute this CIIP Newsletter

>Founder and Editors
Eyal Adar CEO iTcon, eyal@itcon-ltd.is
Bernhard M. Hämmerli, HTA, Initiator and Main Editor
bmhaemmerli@acris.ch
Eric Luiijf, TNO, Eric.Luiijf@tno.nl
Willi Stein, BSI, willi.stein@bsi.bund.de

> Graphics and Layout
Florian Widmer florian_widmer@gmx.net

> Spelling:
British English is used except for US contribution

ECN European CIIP Newsletter

Table of Content

Introduction

European Activities

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events

European CIIP Activities Increase

CIIP activities in Europe accelerate. Six such conferences or workshops of international significance are planned for the next six months.

ECN offers a platform where European efforts in CIIP can be showcased by publishing their programs and papers.

Dr. Bernhard M. Hämmerli

Professor in Information Security
Founder of the executive Master Program IT Security, FHZ
President ISSS / FGSec
bmhaemmerli@hta.fhz.ch
bmhaemmerli@acris.ch

In a few days experts from the EU countries of the CIIRCO project will meet in Prague: September 13-15, 2005. The goal is to establish a common overview of the existing CIIP activities in Europe. Furthermore one person from Israel and US are invited.

The second ECN issue supports this process with various contributions from experts and provides their contact information.

Highlights of this issue

We are very happy that James Clarke explains the actual situation of the strategic EU research agenda for security and dependability.

Europe is investing in CIIP activity.

With the newsletter we provide a public forum for contributions, research units and agencies.

Sandro Bologna (CIIRCO project team member) and Claudio Balducelli point out the urgency for making electrical systems more resilient.

Dana Procházková, host of the second CIIRCO Workshop, discusses her view on C(I)IP, its challenges and CIIRCOs' effort to approach the problem. We are particularly happy that Dana Procházková (Czech Republic) and Mieczyslaw Borysiewicz & Slawomir Potempski (Poland) share their point of view on the most urgent CIP topics from the perspective of a new member in the EU.

John A. McCarthy presents the current CIP program activities in the U.S. His institution is editing the U.S. CIP report, the US equivalent to ECN. The report can be downloaded from: http://cipp.gmu.edu/report/ .

The importance of CIP is emphasized in the United Kingdom. The National Infrastructure Security Co-Ordination Centre explains how it conducts its planning for 10 sectors.

Two research contributions provide a valuable perspective: Geert Deconinck from Belgium proposes a middleware architecture for a dependable info'structure in energy application. Engina Krida, together with Christopher Kruegel, proposes a global security and dependability framework.

The recently founded CIP expert group in Germany was involved with organising the CIP Europe 2005 symposium on September 19, 2005 in Bonn. Dirk Schadt Chair of the expert group reports.

Stephen D. Wolthusen, program chair of the first IEEE CIP international workshop in Darmstadt, November 3&4, 2005, gives an overview of the topics that are to be covered.

Authors for contributions to the future issues of the ECN are very welcome. Please contact me. Further information about the ECN and its publication policies can be found in the introduction to the first issue.

www.ci2rco.org

Enjoy reading the ECN!

.

IST-SecurIST - Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D

Security research framework for Europe - Empowering the citizen.

James Clarke

Mr. James Clarke received a B.E. in Electrical Engineering in 1986 and an MSc. Applied Mathematics in 1992. He works for the Telecommunications Software & Systems Group (TSSG) at the Waterford Institute of Technology in Waterford, Ireland. Mr. Clarke is working as the operations manager on the IST SecurIST project (FP6-004547) and the leader of the Applications Security Initiative (ASI) in the European Security and Dependability Task Force www.securitytaskforce.org.

Europe is heavily investing in research programmes within past and future Framework programmes (FP5-FP7) to establish a solid security and dependability infrastructure. As part of FP6, the IST-SecurIST project, which initiated in November 2004, is a Supporting action project whose goal is to facilitate the delivery of a Strategic Research Agenda for ICT Security and Dependability R&D for FP7. The first step in SecurIST is to establish a European-based Taskforce comprised of researchers and an Advisory Board aimed at defining the foundation for the required future research in these areas. It is critical to the success of the strategic research agenda that the projects and people already engaged in Security & Dependability R&D contribute not just to sharing of knowledge and technology deployment in their specific areas, but also address how their research activity will contribute to higher level issues, and to the elaboration of the Strategic Research Agenda for FP7.

The Security and Dependability Task Force (STF)

The SecurIST project is attempting to achieve a degree of consensus by bringing together lead players in these areas under the Security and Dependability Taskforce. The approach taken was the establishment of themed working groups under the taskforce charged with the task of contributing to the development of a security road map to support future ICT security requirements. The emphasis is on developing common research links between the various themed areas. Following the initial gathering of Security and Dependability experts at dedicated networking sessions at IST 2004 held in The Hague in November 2004, and two highly successful Workshops hosted by the SecurIST project and the European Commission in January and April of 2005, the Security and Dependability Task Force[1] has been established and formally launched.

Following the initial gathering of Security and Dependability experts ...., the Security and Dependability Task Force [1] has been established and formally launched.

The following areas of security and dependability research today have been identified within the following Working groups within the STF:

Wireless Security Initiative (WSI)

This initiative targets security in Mobile/ Wireless service environments. It will address Ambient Radio, Ambient Networks and User Device capabilities in a 3G/3G beyond, Ad-hoc and All IP networks. It will address mobile, wireless and smart card technologies covering the development of new protocols, interfaces, technology interoperability and future standardisation issues in this space.

[1] http://www.securitytaskforce.org

Internet Infrastructure Security Initiative (IISI): Focuses on security models and technologies for GRID, advanced cryptography for multimedia Internet and e-commerce applications, secure software for the future Internet, novel trust and security models for Internet and interoperable ubiquitous computing environment, dependable home connectivity as the advent of ambient intelligence, privacy, authentication, accounting and reliability for Internet.

Application Security Initiative (ASI): Directed at improved and novel approaches to application level security measures. New architectures and end-to-end security design issues to protect at an application level in future networks. The following areas are being investigated: security tools, policies, context management, allowing trusted users to view documents, single sign-on, digitally signing web pages for example, application vulnerability validation, anti-virus and so forth.

Dependability and Trust Initiative (DTI): Concerned with two main issues: the confluence between classical dependability and security, met essentially but not only by the concept of common 'accidental fault and malicious intrusion tolerance'; and the necessary but often forgotten link between trust (dependence or belief on some system's properties) and trustworthiness (the merit of that system to be trusted, the degree to which it meets those properties, or its dependability).

Identity & Privacy Initiative (IPI): Research focusing towards digital identity management, privacy mediation, personal data environments, privacy and authentication within the mobile/Internet environment and so forth.

Security Policy Initiative (SPI): Focusing on research in policy-driven security in the areas of languages and tools and policy-based applications. This approach will let managers concentrate on high-level rules rather than implementation details and provide auditors with a formal specification for measurements.**Security Research Initiative (SRI):** This initiative has a wide spectrum of themes and challenges to be addressed to secure and protect information such as developing new protocols for identification and authentication, interoperability between wired and wireless networks, survivability infrastructures and countermeasures for new attack models such as denial of service attacks.

Biometrics Security Initiative (BSI): interested in new algorithms, alternative solutions, novel pattern recognition approaches, multi-modal biometrics, data fusion issues, standardization of testing bio data and so forth.

Digital Asset Management Initiative (DAMI): Developing novel watermarking and stereophony algorithms, advanced cryptography, standardization of services for digital rights management and payments, securing CD/DVD copyrights, virtual electronic licensing and so forth.

Cryptography Research Initiative (CRI): Focusing on advanced and novel cryptography algorithms, PKI, Digital signatures, increased stream size needed for more efficient and sized cryptographic needs and so forth.

Security Architecture and Virtual Paradigms Initiative (SVPI): Addressing the needs to deliver Framework Solutions Architectures for security enhancement and its testability and diffusabilty evaluation.

Methods, Standards, Certification Initative (MScI): Focusing on methods, processes, certification and standards related to advanced security and dependability.

IPv6 Security & Privacy Initiative (v6SI): This initiative focuses on analysing the new security features IPv6 brings to the table, and compares it to security deployed in legacy IPv4 networks under the presence of Network Address Translation (NAT). It will especially highlight the improvement of the end-2-end model to security and illustrates benefits for fixed and mobile communication. Closely coupled with security, it will also investigate privacy concerns and the solution IPv6 is providing in this area. As a result, roadmaps will be drawn for deploying IPv6 security and privacy solutions in different end-user scenarios, such as for fixed communication, host mobility or ad-hoc networks.

Security and Dependability Advisory Board.

One of the prime tasks and project milestones of SecurIST is the establishment of an Advisory Board of the Security Task Force whose goal is to oversee and consult the STF initiatives in the formulation of the European Security and Dependability roadmap. In parallel with the development of the STF Working Group Initiatives, Advisory Board members were recruited and their kick off meeting was held in June 2007. The STF Advisory Board is comprised of esteemed members of both industrial and academic backgrounds within the ICT Security and Dependability community. The members of the Advisory Board have demonstrated immediate contributions, will and drive and are currently reviewing the initial draft of the Security Research Framework Whitepaper and the STF Initiatives first compiled Document for comments (DFC). The STF is strengthened tremendously by this unique selection of security and dependability advocates thus making it well positioned to deliver on its workplan.

Security Research Framework

ICT is at the heart of the emerging Knowledge Society. Threats are more diverse and less predictable and Europe must develop a framework to ensure a secure EU in a better world. A knowledge society reflecting the cultural and economic needs of the European Community will be greatly assisted through the development of a European security ICT research programme that addresses the following challenges:

- the creation of an EU security culture supported by credible EU industry and research infrastructure;
- development of security and risk awareness by European citizens, businesses and institutions;
- need to develop synergies between civil and homeland security research and between public and private sector;
- in preparing for FP7, Europe must develop the security research agenda whilst creating a technology Pillar in security, which is capable of vertical integration with the key technology platforms;
- developing and implementing Security by Design with European values incorporating citizen's needs as basis for next generation infrastructure and ambient computing;
- development of specific security mechanisms to address the vulnerabilities introduced by new technologies for communications and service provision.

This security research framework must be defined in the context of the emerging networked information society. Citizens and businesses are forming virtual communities based no longer on physical location but rather on common interests and goals. Not only is ICT a part of everyday life but it is an essential part of Europe's easily overlooked critical infrastructure such as emergency services, electricity, oil and gas supply, nuclear power plants and so forth. At the same time as the technology creating this networked society becomes ever more pervasive and essential, it becomes more complex in its structure, and its demands for management and control. The increased complexity arises not only from the growth of the networks and their usage but also from increasing heterogeneity and integration and the consequent dynamics as users move continuously around, and continually switch between services and communications systems.

The pervasiveness of this new technology may be characterised by possibly billions of intelligent devices and components working with and on behalf of citizens, government and businesses. The vision is that these devices will permeate all aspects of the citizen's life, from birth to death, in a seamless non-intrusive manner and, perhaps all but invisible, will benefit the individual citizen and society as whole.

This emerging picture has major implications for the social and economic future of Europe: while the benefits for Europe are enormous, there are also major challenges and potential dangers that Europe needs to be aware of and to act upon if it is to ensure that society maintain its desired stability and progress.

The virtual communities and their individual members, business and societal, need to be able to trust the communications infrastructures and the services that they deliver. The security and dependability of these infrastructures needs to develop and strengthen to keep pace with the increasing dependency on them. Our information society will flourish only if it can offer the same level of trust as traditional methods and services. At the same time, the *usability* of that security has to be taken into account so that users are neither frightened-off nor feel overly burdened. The benefits and value must be seen as commensurate with the apparent costs[2]: financial, performance, freedom-of-action, etc. New vulnerabilities and risks will arise from the increased complexity and dynamics in terms of faulty design and implementation, malfunction, malicious activities and intrusion.

Europe recognizes the need, as stated in the Lisbon strategy agreed by the member states, for the EU to create *"the most competitive and dynamic knowledge based economy in the world, capable of sustainable economic growth with more and better jobs and greater social cohesion"*[3].

To achieve this, Europeans will need to develop trust in the security, privacy and dependability of the technological improvement in the networks and services that are going to deliver the anticipated advances, as Europe leads in the delivery of e-government, e-commerce, e-learning, and e-*infotainment*, etc. We need to move beyond compliance management and policies to Citizen Empowerment in a highly integrated networked and pervasive ICT environment.

Anyone interested in finding out more information or contributing to the Security Task Force can register on **http://www.securitytaskforce.org** .

Acknowledgements

IST-SecurIST (FP6-004547) is a project funded by the European Commission's Sixth Framework Information Society Technologies (IST) Programme, within the Unit ICT for Trust and Security.

[2] the cost of prevention and planned recovery may be large – but finite, whereas cost of a head in the sand, it-may-never-happen, approach is unknown.

[3] http://europa.eu.int/comm/research/era/3pct/index_en.html

SAFEGUARD, a proposal to improve the survivability of electrical power transmission systems

The SAFEGUARD Project placed within the IST Initiative in the 5th Framework Programme of the European Commission addressed the topic of developing an Intelligent Agents Organisation to Enhance Dependability and Survivability of Large Complex Critical Infrastructures

<www.ist-safeguard.org>

Sandro Bologna

Project Manager at ENEA, Modeling and Simulation Unit. He has nearly thirty years experience in the field of computer based systems for safety applications
Phone: +39-06-30483708
E-mail: bologna@casaccia.enea.it

Claudio Balducelli

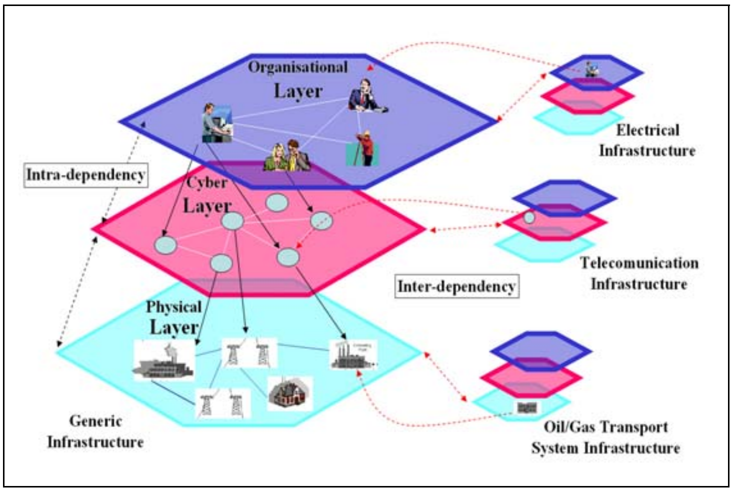
Senior Researcher and Scientific Project Coordinator of ENEA, Modeling and Simulation Unit
Phone: +390630483334
E-mail: claudio.balducelli@casaccia.enea.it

Certain technological infrastructure, such as the electricity power transmission system, are critical for the well being of modern societies, and their protection has been part of national defence planning for decades, thought at different levels of importance. But, if in the past security meant limiting the physical access to the *hot* sites, now day, the so-called information revolution and the new energy market, makes such infrastructures increasingly automated and interlinked, inheriting a variety of vulnerabilities that cannot only be addressed by physical control policies.

Cyberspace, defined by the US Department of Homeland Security as an *interdependent network of information technology infrastructures*, is at the same time the nervous system of our society and its Achilles' heel.

The Critical Infrastructures are today more interdependent that in past. As visualized in the figure these infrastructures are composed of:

- a *physical layer* (the physical equipments and the hardware components),
- a *cyber-layer* (the cyberspace, containing supervisory and control harware and software),
- an *organisational-layer* (the operative management and human organisations cooperation).



The objectives of the Safeguard technology is to improve the dependability and survivability of large complex critical infrastructures by monitoring and protecting them with *autonomous agents* that observe manly the working status of the *cyber-layer*, making on-line diagnostic functions, and performing recovery actions including emergency notification.

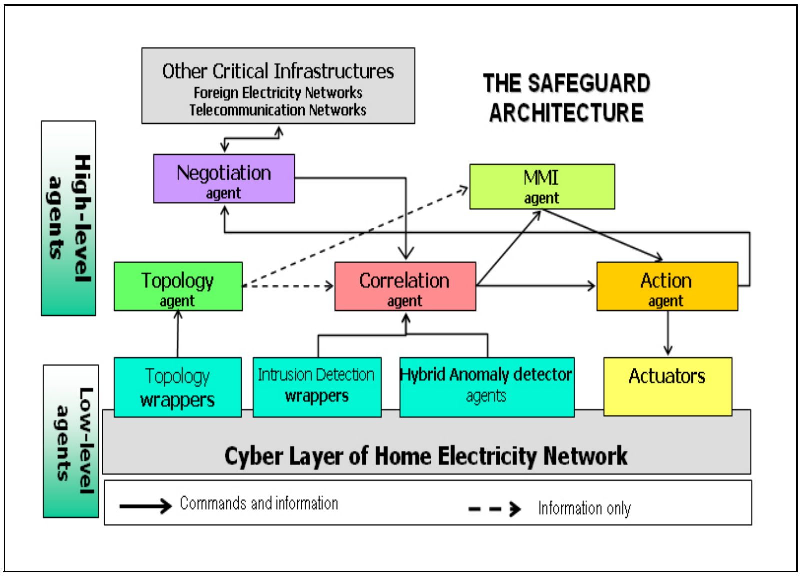
At present the availability and integrity of critical infrastructures are usually monitored and maintained by human operators. Safeguard uses agent technology to improve the capabilities of the automatic control functions while also helping the human operators to make the right decisions at the right time.

The Safeguard Product Description

Safeguard product, whose architecture is visualised in the figure, can be looked at in two different ways:

As an **Integrated Product** implementing an add-on solution to safeguard Large Complex Critical Infrastructures. This is long term goal requiring an integration with existing SCADA systems (Supervisory Control and Data Acquisition).

As a **Suite of Modular Components**: it is possible to exploit the capabilities of some Safeguard agents to solve particular problems that are generally present inside the electricity domain but that could also be common to other domains.


THE SAFEGUARD ARCHITECTURE
Other Critical Infrastructures
Foreign Electricity Networks
Telecommunication Networks
High-level agents
Negotiation agent
MMI agent
Topology agent
Correlation agent
Action agent
Low-level agents
Topology wrappers
Intrusion Detection wrappers
Hybrid Anomaly detector agents
Actuators
Cyber Layer of Home Electricity Network
Commands and information
Information only

The suite components are:

The **Wrapper Agents** which are dedicated to gathering data and pre-filtering information from the Cyber-layer, for different purposes.

The **Hybrid Detector Agents** have two different components. An *anomaly-detecting* component specialising in detecting deviations from normality and a *signature-based* component used for failure alert classification based on earlier knowledge.

Three different types of hybrid detectors are available:

Event course hybrid detector, based on CBR (Case Base Reasoning) technique, was deployed in the electricity network to monitor deviations from normal event sequences within the SCADA control system. It may also be configured and trained to detect anomalies and signature-based failures also inside other types of software systems.

Data and invariant hybrid detectors, based on auto-encoding neural networks, process data readings and detect violations of known approximate-invariants in the electricity network. This is used to support the electricity state estimator to find the state of the system more reliably.

TCPdump detectors based on Data Mining techniques analyse and detect anomalies in the packets captured inside IP networks.

The **Correlation Agent** is responsible for gathering information from the low level agents, coming up with hypotheses about the state of the system and suggesting an appropriate response. It is based on a new knowledge engineering approach that integrates temporal and probabilistic reasoning in a highly modular fashion, and evaluates the state of the controlling network by bringing together all the available information sources coming from hybrid detectors.

The **Action Agent,** based on the workflow technique, is the interface between Correlation Agent and the Actuator, and manages the recovery policies with the aim of intercepting and reduce the number of false alarms.

The **Topology Agent** gathers information about the controlled network - including network components, the connections between them, the importance of each component and the services running on each machine. Its compiled information is provided to the Action Agent, the Correlation Agent and MMI on request.

The **MMI Agent** is the major interface to the human administrators. Its primary role is to ensure that all information is transferred and correctly filtered to avoid information overload. In the case of alarms, it proposes possible solutions if the Action Agents are incapable of resolving the situation.

The **SCADA emulator** connected to a load flow electrical simulator acts as data source and operative environment to demonstrate and test the functionalities of Safeguard.

The **Attack Tool** is used to configure a set of attacks against the emulated SCADA system . A tree model has been adopted for the logical description of the attack sets where an attack set, or scenario, is a group of attacks that belongs to an aggression context.

The integration of Safeguard agents inside SCADA systems

In the following figure a general schema is shown which illustrate how to integrate Safeguard agents inside a real SCADA system.

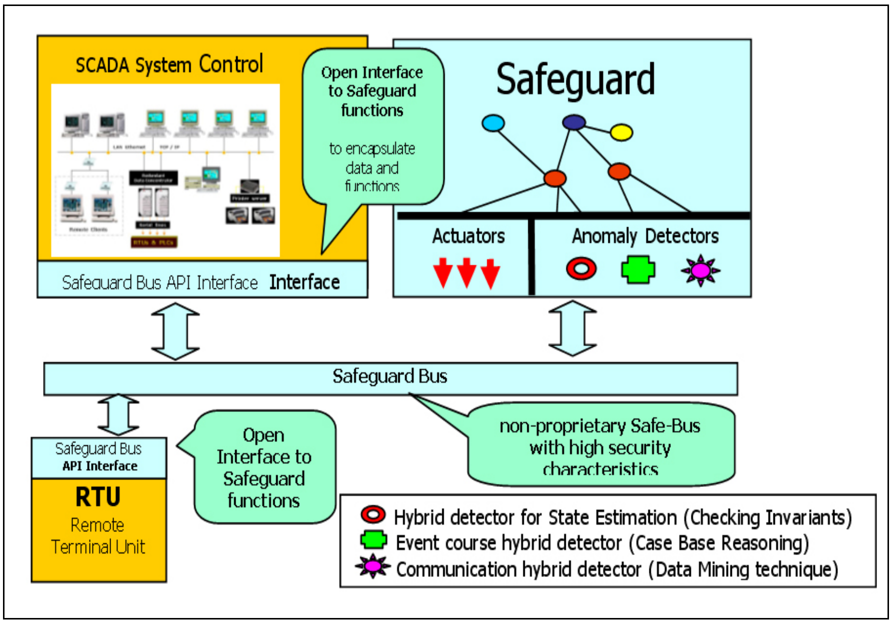
All of the Safeguard agents must be contained inside a separate workstation. The communication channel between the Safeguard agents and applications residing in the Control Centres and in the Remote Units must be a *Safeguard Bus*, i.e. a non-proprietary type of Bus having high security characteristics. A certain set of API (Application Process Interfaces) modules based on *cryptographic material* must be dedicated to encoding/ decoding the data contents.

High Level Safeguard Agents do not communicate directly with the Safeguard Bus. Only low level agents and actuators are responsible for acquiring data and sending commands to the Bus, utilising a special crypto-graphic communication mechanism.

To insert this type of improvement, a re-engineering phase is needed involving the communication mechanism between low level agents and SCADA components. In practice, the low level agents already utilise a special interface called *instrumentation* to exchange data with the SCADA Emulator; to make the integration it is necessary to modify this interface, introducing all the necessary functions.

The Safeguard solution for the electrical power transmission systems has been extensively tested using a Testbed implemented in the ENEA Labs at Casaccia Center, based on an Electrical System Simulator and a SCADA System Emulator. The results have been promising and the System is evolving towards a more mature stage.

Future Developments


SCADA System Control
Open Interface to Safeguard functions
to encapsulate data and functions
Safeguard
Actuators
Anomaly Detectors
Safeguard Bus API Interface Interface
Safeguard Bus
Safeguard Bus API Interface
RTU
Remote Terminal Unit
Open Interface to Safeguard functions
non-proprietary Safe-Bus with high security characteristics
Hybrid detector for State Estimation (Checking Invariants)
Event course hybrid detector (Case Base Reasoning)
Communication hybrid detector (Data Mining technique)

In the future it is intended to improve the effectiveness of already developed Agents as well as to develop new ones introducing a *self-awareness* capacity i.e. the capacity to understand if themselves or the external environment, in which they lives, are changing or not; in such way should be reduced the number of *false alarms* that are often unacceptable. It is intended also to improve the agent's capability to *optimise* their behaviour in relation with the modification of the environment in which they operate, making use of some *genetic/biological inspired* algorithms.

Invitation for Cooperation

Industrial organisations and universities are invited to cooperate to develop usable models to simulate system breakdowns and alternative courses of action as well as to indicate the future path for research.

Cooperation is also encouraged to enhance the capabilities of the current Safeguard system in the areas of distributed awareness, supervised and unsupervised alarm correlation, optimisation, self-healing and human decision support.

Next step will be to investigate, together with SCADA systems providers, the possibility to integrate Safeguard agents inside a real SCADA system.

About the SAFEGUARD Consortium

The partners in the SAFEGUARD project were:

- Queen Mary, University of London (**UK**)
- Applicaciones de Informatica Avanzada (**Spain**)
- Italian National Agency for New Technology, Energy and the Environment (**Italy**)
- Linkoping University (**Sweden**)
- Swisscom Innovation (**Switzerland**)

Some Problems of Critical Information Infrastructure

Tasks like CIIP are trans-national and trans-disciplinary. Therefore the exchange of information should be fostered. ECN is a platform to communicate CIIP related activities to provide networking possibilities for CIIP experts and stakeholders. We hope it serves its purpose.

Dana Procházková

CITYPLAN Ltd. Praha,
Czech Republic
CIIRCO Project

1. Introduction

The fundamental function of the state is to ensure the existence and sustainable development of human system / space, which is not possible without ensuring the safe space for human society. The safe space is a space in which the safety level is acceptable and in which sustainable development is guaranteed. With regard to present knowledge the safety must be mainly considered in integral sense and with regard to protected (safeguard) interests that are:

- human lives, health and security,
- environment,
- property and welfare,
- technologies and infrastructures, mainly critical ones.

Critical infrastructure are physical, cyber and organisational subsystems of human system that are necessary for protection of human lives, health and security, property and minimal function of state economy and administration. They create potential for putting under control all critical situations that are possible in human system. Analysis and evaluations performed show that the attention paid to critical cyber infrastructure is not on the required level.

2. Disasters and Emergencies

At selection of the strategy for security there is necessary to take into account a broad set of disasters and the reality that new disasters will grow during the time from many reasons. The disaster is a phenomenon that leads or can lead to damages and harms on protected interests of the state. Today, we know that we must minimally take into account the following disasters:

- *natural disasters:* landslides, hot summer days, drought, dam rupture, floods, tsunami, earthquake, volcanic eruption, slope sliding, rock sliding, wild fires, winds, tornadoes, hurricanes, extreme rainy or snowfall precipitations, gas releases of the Earth's interior,
- *technological disasters:* incidents and accidents in chemical and other industry, induced earthquake (rockbursts, shocks induced by dams, by injection of fluids into the Earth's interior, pumping the fluids from the Earth's interior, artificial explosions), accidents at transporting and stocking the chemical materials, traffic accidents, radiation accidents and big environment pollution's,
- *disasters directly influencing the balance of human population and society, environment and critical infrastructure:*
  - defects in environment: collective pestilence's of field culture, collective pestilence's of animals,
  - defects in human population: epidemic and pandemic, human faults,
  - defects in human society: the defects in public security and public order, abasement, discrimination, criminality, terrorism, wars, armed conflicts,
- defects in critical infrastructure: the defects in economic sphere, territorial, organisational and social infrastructures, in information technologies, communication, energy sector and banking.

At the disaster occurrence there are originated chains of undesirable phenomena (impacts, consequences) of external and internal character, primary and secondary, which affect negatively protected interests of human system in different intensities and in different time moments. The substantial role plays the local vulnerability and pertinent faults in human behaviour or management on all levels.

To put under the control the originated emergencies there is necessary to understand disaster impacts and to know all links and flows in human system that escalate or suppress disaster impacts. A big role plays interdependencies across the human system or across infrastructures that can under special conditions create undesirable couplings. Sources of such interdependencies are information networks, management tools, finance flows and electric energy networks etc.

3. Open Problems of Critical Information Infrastructure

At present there are technical standards and norms for technology vulnerability reduction, health standards for human population vulnerability reduction, environmental standards for environment vulnerability reduction and legal rules for human society vulnerability reduction, and there are not qualified standards for cyber infrastructure vulnerability reduction. This shows the first domain to which critical information infrastructure protection must concentrate its effort. It is necessary to ensure the protection against:

- technological accidents in information technologies,
- errors or failure of information technology management systems,
- human errors,
- natural disasters or technological accidents of systems on which the information technologies are dependent,
- terrorist attack, criminal acts or war.

Problems connected with information infrastructures are complicated because each information infrastructure consists of elements and networks and protection of networks is always complex, see the long history of effort with security of supplies of electricity, water etc.

The aim of critical information infrastructure protection is at consideration of all above given sources of information technologies failures to arrange in order that the information infrastructures might fulfil required functions at all conditions (normal, abnormal and critical) and to prevent in order that they do not perform operations that are prohibited because they can evoke other impacts on human system, especially on human security. It means that it is necessary to implement into practice the required technical, legal, management, economical and educational measures that secure the information infrastructure reliable operation at design conditions and to codify the appurtenant obligations.

To this purpose there is necessary to map the possible problems of existing information technologies that result to inconvenient impacts on human system. From the safety management point there is necessary to pay attention to critical information infrastructures. For their reliable function there is necessary to codify rules for selection and designing the suitable information infrastructures, for building and operation the information infrastructure. This is not all, because each infrastructure fails or can fails earlier or later, and therefore, the rules for emergencies must be also prepared.

From the viewpoint of human security there is another situation that must be considered in the critical information infrastructure protection. From the disaster investigation it follows that all standards ensure the human system safety only to some level of disaster size, e.g. in Central Europe in the case of earthquake up to the 6° MSK-64 earthquake impact size, in the case of floods up to the hundred years flood level etc. If disaster size is greater than such limit, e.g. in some region are the 7° MSK-64 earthquake impacts or flood has the 150 year flood level, we observe the situation given in figure 1. Figure shows that only nuclear technologies are protected against such disaster size due to the IAEA and the NEA / OECD long-term effort. By arrows there are denoted severe disaster impacts that lead to relevant detriments, losses and damages. Green ones show relevant impacts against to which there are prepared countermeasures mitigating them. Blue ones show relevant impacts for that there are not prepared the mitigative measures in advance. Yellow ones denote impacts that have not been systemically solved yet. Special attention is paid to critical information infrastructures, i.e. important arrows are denoted by bold lines. Because these have not been documented yet, they are solved ad hoc. Just these interdependencies in human system escalate as a rule disaster impacts on human lives, health’s and security because caused secondary impacts and elongated the emergency.

The figure shows that the information infrastructure is one of the sources of secondary impacts on human lives, health and security. I.e. it reveals the second domain to which critical information infrastructure protection must concentrate the effort. It means that information infrastructure must be resistant against all possible disasters at site and that the emergency plans for critical information infrastructure must be compiled, at least in the form of continuity plans.

It means that for human security there is necessary to define the concept of human safety in which there will be considered not only direct impacts but also impacts mediated by complex network of links existing in human system. The critical information infrastructure must be especially considered in this concept.

4. Conclusion

The information infrastructures are used in many systems and subsystems of other infrastructures, which belong to the human system. From the viewpoint of their protection we must ensure in order that they credibly operated not only at normal and abnormal conditions that are covered by their design, but also at emergency conditions developed by various causes. Attention must be concentrated to critical information infrastructures, which cause big direct impacts on the human lives, health and security or which can escalate disaster impacts on the human lives, health and security. With regard to a great multiplicity of information infrastructure types, there is necessary for human security and human system safety in the first to map the situation and to recognise problems, i.e. to determine:

Which conditions are required, that the information infrastructures will fail, and why will it fail?

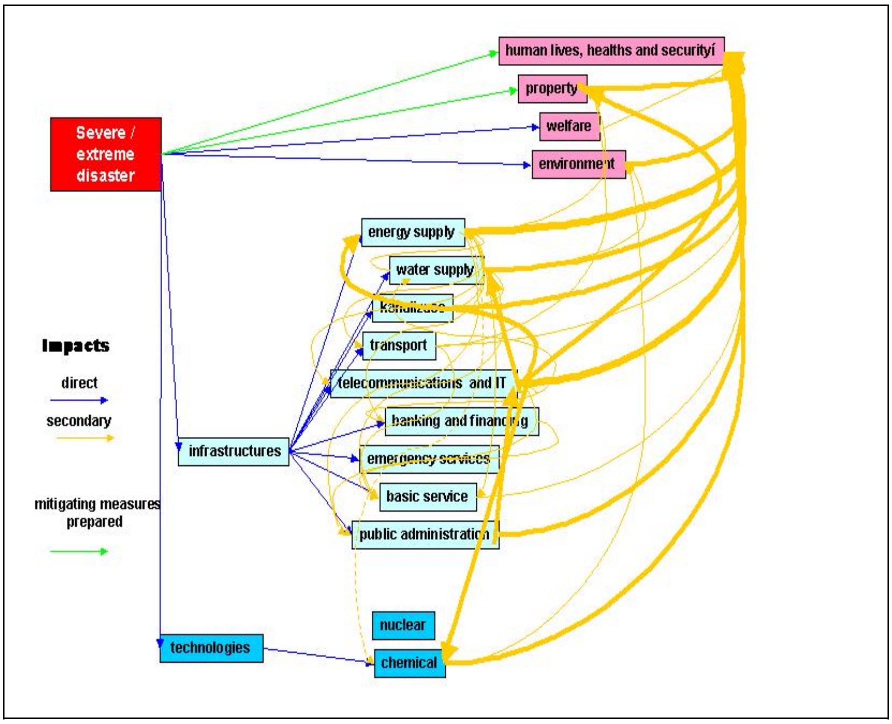


Fig. 1: Impacts of severe / extreme disaster on protected interests with regard to standards in force in Europe. Special attention is paid to critical information infrastructure – bold lines.

- What impacts on human lives, health's and security can the information infrastructures failures cause?
- Which measures can suppress the information infrastructures failure occurrence or which measures can mitigate the information infrastructures failure impacts on human lives, healths and security?

The CI2RCO project is just the project that surveys the situation in the EU member countries and in their surroundings. Analyses, performed till now, disclosed the gaps in understanding the problems associated with critical information infrastructures and in ways of their solving; in practice they are solved by the ad-hoc way. Because operative solution are mostly short-term, there is necessary the research effort to concentrate to strategic solution findings. For this purpose there is necessary to establish required aims of critical information infrastructure protection and to co-ordinate the effort of all research teams to implementation of these required aims.

The CI2RCO project is going to contribute to solution of tasks associated with the critical information infrastructure protection, hence it is very important. Therefore, there is necessary systematically to create conditions for the fulfilment of tasks that are given in its assignment.

The Critical Infrastructure Protection Program

Building an Interdisciplinary Critical Infrastructure Protection Program in Academia

John A. McCarthy

Director and Principal Investigator, Critical Infrastructure Protection Program George Mason University School of Law

Universities play a vital, if often overlooked role in supporting the national agenda relevant to homeland security. While always a significant contributor to research and development initiatives, the ever changing landscape of threats and vulnerabilities requires a swift response on the part of academia to produce not only research, but also new generations of graduates ready to step into various positions related to homeland security. The introduction of the Department of Homeland Security (DHS) sponsored Homeland Security Centers of Excellence and the individual programs that have organically grown within universities throughout the US are uniquely positioned to harness fragmented and departmentalized capabilities into interdisciplinary and collaborative research projects, allowing innovative solutions to complex problems with greater speed than traditional research models.

Creation of the CIP Program

The Critical Infrastructure Protection (CIP) Program is congressionally sponsored and uniquely situated at the George Mason University (GMU) School of Law in Arlington, Virginia. Conceptualized and organized prior to September 11th 2001, the CIP Program has been operating as a defacto DHS Center of Excellence focused on infrastructure protection and public-private partnership. Built upon a strong foundation in law, policy and technology, the CIP Program seeks to enhance the security of cyber-networks, physical systems, and economic processes supporting the nation's critical infrastructures through an interdisciplinary research agenda. With the National Institute of Standards and Technology, of the Department of Commerce, serving as its executive agency, the CIP Program funds basic and applied research, as well as supports information and outreach activities related to key components of the national research agenda. During the past three years, the CIP Program has sponsored interdisciplinary and multi-institutional research within virtually every academic unit at GMU and nearly two dozen universities nationwide, including prime partner James Madison University in Harrisonburg, Virginia. This research has spawned multiple books, including *Critical Infrastructure Protection Program Workshop I Working Papers* and *Workshop II Working Papers* and a soon to be released oral history of critical infrastructure protection (coming fall of 2005). In addition to many policy papers, over 270 scholarly publications have been placed in peer reviewed journals and presented in national and international forums.

The CIP Program serves as a nationally recognized Center of Excellence for infrastructure protection and public private partnership.

In addition to basic and applied research activities, the CIP Program maintains an extensive outreach effort to highlight and advance current topical issues relevant to the national agenda. Our acclaimed *Critical Conversation Series*, held at the National Press Club in Washington, DC, and moderated by CNN Whitehouse Correspondant Frank Sesno, convenes leaders from the executive branch, Congress, industry and international organizations to discuss issues relevant to CIP. Recent events have included *Getting Serious About Cybersecurity* (June 2005) and *Turning the Tide, Securing America's Ports* (July 2004). In addition to these high profile events, the CIP Program also hosts numerous workshops, seminars and conferences, focused on technology, law, economic and policy areas, and quietly convened sessions of government and private sector leaders at the behest of an outside stakeholder. Building upon this outreach and engagement strategy, the CIP Program also publishes *The CIP Report*, a monthly, electronic newsletter for professionals in industry, government, and academia who have an interest in critical infrastructure protection. Beginning as a small publication catering to those familiar with the field, the newsletter has grown to an international distribution and provides informed and timely discussion regarding the latest information about emerging legislation, government initiatives and leaders, and academic endeavors and is available online.

Three core principles of the CIP Program: interdisciplinary, multi-institutional and in support of the national agenda

Among the many topics explored, key areas of focus have been cyber security, physical security, information sharing between public and private sectors, regional, state and local issues, and privacy concerns. As the project expanded, ongoing activities were leveraged to generate new funding that matured the project scope to address unexplored areas of critical infrastructure protection. By 2004, the CIP grant had evolved into a family of projects under the overall umbrella of the CIP Program.

The CIP Program Model

The CIP Program operates on three core principles: first, research must be interdisciplinary, reaching across all academic disciplines; second, research must be multi-institutional as no one institution has the capacity or depth to address all problems; and, finally, the needs of the national agenda must dictate where attention is focused. We believe that these principles, when integrated, truly leverage the theoretical and intellectual capacity of the scholarly community with the practical needs and problems articulated by government and private stakeholders.

The CIP Program has enjoyed considerable success in harnessing the wide-ranging capabilities of multiple institutions, while selectively engaging researchers and universities around the country to input into projects and initiatives. Based upon the work already underway, the Private Sector Programs division of the CIP Program was established in December 2003. The Private Sector Programs group provides analytical, academic and administrative support related to cross sector and interdependency issues facing private sector owners and operators of critical infrastructure, and helps manage the interface with appropriate Department of Homeland Security program elements. This work focuses legal, economic, business and cultural solutions to enable the private sector to enhance critical infrastructure protection both through private initiatives and working with the government. The Private Sector Program group provides secretariat assistance to private industry Sector Coordinators, Information Sharing and Analysis Centers and other groups with respect to Homeland Security issues. This program is funded through a separate contract with the Department of Homeland Security's Information Protection Directorate.

In addition to the Private Sector Program, the CIP Program expanded to include the National Capital Region (NCR) Critical Infrastructure Vulnerability Assessment Project in March of 2004. George Mason University, under grants from the Urban Area Security Initiative and the Department of Justice Community Oriented Policing Program, founded the NCR Project and partnered with five additional universities in the National Capital Region, which includes the Commonwealth of Virginia, the State of Maryland and the District of Colombia. Aligned with the National Infrastructure Protection Plan, the NCR Project focuses on developing methods to inform public and private decision-makers on the benefits and cost of initiatives to enhance the security of the region.

Keys to Success

The CIP Program has enjoyed considerable success, measured by the substantial growth in not only projects, but in the expertise of people who have joined the staff over the past three years. While this success is reflective of the quality of research and work generated, it has brought with it unique challenges that have required innovative solutions. Program success is dependent upon an ability to quickly respond to changing priorities on the part of sponsors and current developments in national security, lending an entrepreneurial quality to the Program's work which is rarely found in an academic environment. Fortunately, another critical component of success has been the overwhelming support shown by the administration of

George Mason University, enabling the CIP Program to rapidly grow and expand, while encouraging collaboration across the university.

Perhaps even more critical to the overall success of the Program is the emphasis placed on partnership and collaboration. To be truly interdisciplinary requires not only strong networks and relationships throughout George Mason University, but with partners in universities around the country. The multi-institutional nature of the CIP Program not only affords the opportunity to engage the best and brightest researchers available, but builds new connections between researchers with complimentary research projects. Each university brings distinct capabilities that strengthen the Program as a whole and pre-existing relationships enable the CIP Program to respond more quickly to new inquiries and opportunities.

Next Steps

As the CIP Program enters its fourth year, we have begun to refine and adjust the model that has served so well. While we continue to fund research throughout this and other universities, we have also added more talented researchers to our core staff, affording us the opportunity to quickly produce policy papers on issues that have emerged as a result of other research activities or to partner with new groups to host conferences and symposia in unexplored areas of critical infrastructure protection.

One area of increasing activity and enagement for the CIP Program is international issues facing the critical infrastructure protection community. While we have been active in a number of conferences and publications, each presenting new opportunities for engagement, we welcome new avenues for collaboration and partnership.

As previously mentioned, this fall marks the release of an oral history of critical infrastructure protection in the United States. This project will document the history of critical infrastructure protection through primary and secondary sources. The final version of the project provides analysis of CIP from the earliest days of the United States to a detailed look at its evolution since 1997. Interviews with people from both the public and private sectors, with hands-on roles in developing CIP, were conducted over a year and a half's time. The resulting product found a number of themes throughout CIP history, including the inherent difficulties in protecting infrastructure that is more than 85% owned by the private sector, the simultaneous benefits and vulnerabilities that the cyber revolution has introduced into critical infrastructure, and the daunting reality that deliberate attacks, accidents, and natural disasters can have devastating and cascading effects on this networked system of infrastructure that knows no boundaries.

Another avenue of continued development and expansion for our Program is our newly constructed web site. While we have maintained a web presence since the earliest days of our Program, in April 2005 we launched a newly designed site that will provide greater opportunity to showcase the many projects currently underway at the CIP Program. We will continue to build our CIP library, which contains a searchable database of documents foundational to CIP, all past and current issues of *The CIP Report*, working papers from recent conferences and events, and will soon link to the transcripts and resources used to compile the oral history publication.

For more information about the CIP Program, please visit our web site at http://cipp.gmu.edu.

GEORGE MASON UNIVERSITY | School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

NISCC: minimising the risk of electronic attack to the UK CNI

Society today is complex and interdependent. We all rely on vital computer networks for our day to day existence. ECN looks at the work of NISCC - the UK's electronic defence agency.

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

www.niscc.gov.uk
enquiries@niscc.gov.uk

+44 (0)870 487 0748

The Creation of NISCC

On 20 December 1999 the UK Home Secretary announced the creation of the National Infrastructure Security Co-ordination Centre (NISCC).

NISCC is an interdepartmental organisation set up to co-ordinate and develop existing work within UK Government departments, agencies and organisations in the private sector, to minimise the risk of electronic attack against the UK Critical National Infrastructure (CNI).

The UK Government views the CNI as *'those assets, services and systems that support the economic, political and social life of the UK, whose importance is such that any entire or partial loss or compromise could:*

- *cause large scale loss of life;*
- *have a serious impact on the national economy;*
- *have other grave social consequences for the community or any substantial part of the community; or*
- *be of immediate concern to the national government'.*

The UK CNI consists of the following 10 sectors:

Communications
Emergency Services
Energy
Finance
Food
Government and Public Service
Health
Public Safety
Transport
Water & Sewerage

NISCC draws on resources from across government. Defence, Central Government Policy, Trade, the Intelligence Agencies and Law Enforcement all contribute expertise and effort.

NISCC has no regulatory, legislative or law enforcement role; it seeks to minimise the risk to the CNI through its four key business strands:

Response
Outreach
Threat
Research and Development

Reponse

The NISCC Response group was formed to meet the threat of electronic attack against the vital networks of the CNI.

The Response group employs highly skilled specialists who undertake the technical incident response management of electronic attack problems encountered by the NISCC community. It has extensive links with agencies within government and the commercial environment, both in the UK and abroad.

The group incorporates UNIRAS, the HM Government Computer Emergency Response Team (CERT). UNIRAS provides government and CNI organisations with support in responding to electronic attack incidents. This may vary from answering queries via the telephone to onsite assistance provided by NISCC Response Group specialists.

Team members are specialists in the field of IT Security Incident Management and besides their normal day-to-day activities regularly lecture in incident management on courses for the NISCC community. They also provide assistance to other organisations wishing to set up Incident Response Teams.

CNI partners have chosen to work with NISCC in a mechanism known as an Information Exchange.

UNIRAS has extensive international contacts in the field of Incident Management and works with them to combat global security incidents such as virus infections and hacking attacks. UNIRAS is also a member of the Forum of Incident Response and Security Teams, and the European Task Force — Computer Security Incident Response Teams (TF-CSIRT). It is also a Trusted Introducer Accredited Team, a scheme established to formalise trust relationships between CERTs and facilitate more effective incident management.

NISCC works with government departments and agencies, commercial organisations and the academic community to research vulnerabilities and potential threats to IT systems, especially where they may have an impact on the CNI. It also co-ordinates the public disclosure process where a particular problem extends across a number of software products.

IT security incident management encompasses a number of different skills at both technical and non-technical level including problem identification, analysis, resource handling, forensics, intelligence gathering and project management. It entails talking to vendors and academia about highly technical issues, in-depth analysis of hardware and software configurations, and extensive research.

Outreach and the Information Exhange model

NISCC's Outreach Team works with organisations within the CNI to ensure that their critical IT systems are adequately protected from electronic attack.

The sharing of information about the risks facing networks is self-evidently beneficial to both government and industry. If a mechanism can exist through which one company can learn from the experiences, mistakes and successes of another, without fear of exposing company sensitivities to competitors and the media then every participant can improve their level of assurance.

Thus CNI partners have chosen to work with NISCC in a mechanism known as an Information Exchange (IE).

IEs depend upon the personal trust of representatives. Meeting face-to-face, in a confidential environment results in a trusted, relatively small community with a common interest. Each organisation within an IE can put forward a maximum of two representatives and cannot send substitutes as this would inhibit the sharing of sensitive information.

In addition to the Exchanges facilitated by NISCC, other exchanges will be set up, both in the UK and internationally. NISCC is creating channels through which information in one Exchange is passed to others; there exists such a channel between the UK and US Network Security Information Exchanges.

So far NISCC has facilitated the creation of six Exchanges, and hopes more will be set up this year.

Threat

NISCC's key role is to minimise the risk of electronic attack to the CNI. This involves assessing ’threats’ from a variety of sources including criminals, foreign intelligence services, terrorists or virus writers.

NISCC assists CNI providers in assessing the risks they face and helps them determine the measures they need to put in place.

Companies are, for example, asked to examine their own profiles and the information they expect to hold. By determining the extent of the risk they face, decisions can be taken on the measures required to ensure systems are adequately protected.

NISCC's threat assessment capability is sophisticated; drawing on open source material, sensitive intelligence from home and abroad, and direct contact with those who have experienced electronic attack (eA). There is a high degree of trust within the NISCC community and this information is protected at all times.

Research & Development

The work of the NISCC Research and Development Programme is structured into three strands:

Studies – short tasks to support issues raised by NISCC business activities.

Research – mainly focussed on investigations into new threats and vulnerabilities that may prove to be challenges for the NISCC community.

Development - generation of a capability, either as technical tools resulting from research or processes needed by either NISCC or its community.

Information Sharing

In order to stimulate better promulgation of alerts and warning, to improve awareness and education and to encourage incident reporting, NISCC promotes three types of Information Sharing model which address the threat from an electronic attack against information systems. As discussed above CERTs and Information Exhanges play an important role in these efforts. Another recent addition to NISCC's Information Sharing programme is the Warning, Advice and Reporting Point (WARP) initiative.

Warning, Advice and Reporting Points (WARPs)

NISCC recognises that CERTs can require extensive financial and technical staffing resources, and such costs are not viable for many communities who nonetheless would benefit from CERT-type services and support. NISCC has consequently developed a new model, similar to a CERT, but realisable at a fraction of the cost. This alternative concept, which is better suited to the needs of small communities, including SMEs and citizens, is the Warning, Advice and Reporting Point (WARP).

WARPs peform some of the tasks of CERTs but are not expected to provide the technical response directly. A WARP provides to its community a service of early warnings of alerts and vulnerabilities, specifically tailored to its needs. This can avoid the duplication of each member sorting through dozens of sources, or even worse, not having time to monitor developing threats. The WARP also provides a limited help-desk service for the community, geared to the specialised needs and building on the knowledge of the community membership. It also provides a trusted focus for incidents and attacks to be reported, to help find assistance or co-operation in dealing with the problem. Such reports will be valuable to members, but when sanitised and anonymised sharing them with other communities can be equally valuable and will encourage reciprocal Information Sharing.

NISCC assists CNI providers in assessing the risks they face and helps them determine the measures they need to put in place.

Further information on WARPs, including guidance on setting up a WARP, can be found at www.warp.gov.uk

IT Security Awareness for Everyone (ITsafe)

Launched on the 24th February 2005, IT Security Awareness for Everyone (ITsafe) is a new UK Government initiative to provide both home users and small businesses with high quality, plain English advice to help protect personal technical devices (such as computers and mobile phones) from attacks by outsiders.

The ITsafe website issues alerts of the latest viruses and threats as well as general electronic security advice. Users can also sign up to have alerts sent directly to their email address or mobile phone; this service is free of charge.

ITsafe is managed on a daily basis by the Central Sponsor for Information Assurance as part of their contribution to the NISCC programme of work. Responsibility for the technical content and timing of ITsafe alerts rests with the NISCC Response team.

For further information on the ITsafe initiative see www.itsafe.gov.uk

For further information on the work of NISCC see www.niscc.gov.uk

All press enquiries should be directed to:
Home Office Press Office
Tel: +44 (0)20 7035 4381

Critical Infrastructure Protection: actions to be implemented shortly.

Collected list of principal tasks for the implementation of critical infrastructure protection to be accomplished in short-term period in Poland.

Mieczyslaw Borysiewicz
Slawomir Potempski

**Centre of Excellence MANHAZ
Management of Health and Environmental Hazards, Institute of Atomic Energy, PL
http://manhaz.cyf.gov.pl**

Critical infrastructures are physical and cyber-based systems essential to the minimum required operations of the economy and government. They include telecommunications, energy, banking and finance, transportation, chemical industry, water and sewage systems and emergency services, both governmental and private. Many of the critical infrastructures have become increasingly automated and interlinked. These have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. The increased focus on intentional acts requires enhanced risk assessment methods, protection strategies, and response planning. The interdependencies among critical infrastructure sectors also pose particular challenges for government, industry, and citizens in reducing physical vulnerabilities and protecting valuable assets.

The problem of critical infrastructure protection can be structured as follows:

- Assessing risks and vulnerabilities;
- Infrastructure modeling and analysis - simulating and analyzing energy distribution, transportation networks, and other infrastructures;
- Developing and managing infrastructure projects;
- Conducting communication /outreach to improve safety and security awareness;
- Developing regulatory approaches and public-private partnerships that cost-effectively implement government programs;
- Creating secure information management systems;
- Developing emergency management plans and exercises.

Framework of critical infrastructure protection

There is a number of principal tasks associated with all the areas mentioned above. The collection of short term tasks relevant for diagnosis of situation, awareness rising, knowledge dissemination and setting up cooperation networks is listed below. The list is based on a number of WWW materials.

Critical infrastructures are physical and cyber-based systems essential to the minimum required operations of the economy and government.

1. Risk and Vulnerability Assessment

- Identify hazards and vulnerabilities and their potential consequences;
- Assess the likelihood and magnitude of risks;
- What is the reason: accidental or intentional events;
- Develop a strategy and action plan to reduce risks;
- Define processes and measures for verifying;
- Evaluating the management of risk.

These tasks are to evaluate the risks in key areas of physical infrastructure and focus their staff and financial resources on the most serious concerns.

2. Infrastructure Modeling and Analysis

- Electricity, natural gas, and water supply systems;
- Dispersion, fate and transport analyses of toxic substances;
- Environmental impact;
- Transportation modeling (by road, rail, water, pipelines), including hazardous material transport risk analyses;
- Regional economic impact analyses;
- Microeconomic analyses for capital budgeting and activity-based costing.

These tasks are to facilitate assess issues critical to energy and other critical infrastructure systems. It is crucial to maintain some of the most advanced modeling, simulation, and forecasting tools, as well as software and associated databases. A wide range of critical infrastructure analyses should be performed.

3. Outreach and Awareness

- Support a range of private and public sector clients in implementing integrated campaigns that include awareness research, public relations, education, and marketing to achieve social goals;
- Develop crisis communications scenarios for public officials during emergencies.

Strategic communication is an essential component of emergency preparedness. Building and sustaining public awareness of potential threats helps deter events, minimize loss and damage, and improve readiness.

4. Information Management and Security

- make understanding the importance of creating interoperable, adaptable, and secure information systems for collecting, analyzing, and sharing meaningful information;
- help organizations to improve their information management in particular expertise in designing and developing secure, Web-based information portals that support coordinated domestic and international response;
- design and develop the Domestic / International Emergency Response Information Service portal – secure, single sign-on, Web-based information service that provides a common operational picture to support coordinated Domestic / International emergency response

Information and communications systems are key assets within the realm of critical infrastructure.

5. Emergency preparedness, training and exercises

- Develop emergency plans accounting for peculiarities of crisis situations resulting from acts of terrors;
- Validate plans and training for realistic scenarios;
- Develop training programs;
- Teach responders their roles and responsibilities;
- Facilitate/control exercises and conduct follow up to capture lessons learned and developing action plans.

Emergencies present unanticipated challenges and highlight gaps in the planning and response process.

6. Regulatory Solutions

- Assess regulatory solution in force;
- Propose effective enforcement of the regulations.

Protecting national and international key assets and critical infrastructures is a shared responsibility that requires both regulatory actions and market-based incentives to encourage private-sector security measures. The complexity and interconnectedness of different security issues require the broad perspective.

Tasks for different sectors in the area of vulnerability, risk assessment and management to be accomplished in short term

We have collected the most important tasks for different sectors.

1. Chemical Industry Safety

- help identify potential weak points for industries such as chemical plants, oil refineries, and other manufacturing plants that store or process materials that could potentially cause environmental disasters;
- develop contingency plans to eliminate or mitigate dispersion of contaminants that could cause acute and chronic exposure and destruction of critical resources and sensitive ecological habitats;
- risk and process hazard analyses at various chemical and manufacturing facilities including petroleum refineries, pipelines, terminals, and manufacturers of heavy equipment, medical devices, consumer products, and chemicals;
- develop guidance to help facilities determine the off-site consequences of fires, explosions, and releases of toxic chemicals to better determine the risk involved in chemical operations;
- develop cyber security guidance documentation;
- develop guidance for addressing cyber security as part of an overall site vulnerability assessment;
- develop process control security practices and standards;
- implement a voluntary benchmarking of industry participants' current cyber security management practices;
- develop a vendor partnership program with key cyber security solution providers,;
- implementation of a proactive industry outreach to generate awareness, understanding and participation in this global chemical sector initiative

2. Energy Security

- extend techniques for applying existing vulnerability and risk assessment methodology to terrorist attacks to anticipate and evaluate system-wide (energy generation, transmission, and distribution) risks of terrorist attack;
- perform bottoms-up analyses of the energy infrastructure in order to assess vulnerabilities, develop hazard protection plans, analyze economic impacts of energy disruption, and develop mitigation plans to restore energy services;
- analyze detailed power flows on the electric transmission and distribution grids and assess interregional supply constraints and develop detailed models of natural gas production and transportation, and oil disruption analyses that allows to assess vulnerabilities and develop mitigation strategies;
- vulnerability assessment to determine the susceptibility of the energy infrastructure to a terrorism attack that could result in power grid disruptions

3. Water distribution and waste water systems

- develop of methodologies and tools for the security assessment of water utilities;
- carry out a systematic analysis of existing and emerging threats;
- assess vulnerability of water utilities. develop/assess early warning,

response systems to detect and contain contaminants and crisis communications

4. Transportation Security

- develop a comprehensive approach to assessing threats to the security of transportation's physical and information infrastructure
- assisting transportation managers or agencies in performing security assessments, utilizing recommended methodologies;
- developing customized transportation security plans to formalize the strategy for implementing the recommended countermeasures;
- awareness training for local transportation organizations and emergency responders;
- proposing countermeasures, which may include physical and non-physical actions taken to deter or prevent a terrorist incident or to mitigate the damages in the event of an incident

5. Geotechnical Safety

- identify vulnerabilities of critical infrastructure related to unstable soil structure, liquefaction potential, unstable slopes, and exposed tunnels or caverns that may provide an opportunity to maximize their failure consequences due to an act of aggression;
- assesses dam safety;
- design risk assessment methodologies for evaluating and prioritizing dams in the national inventory to focus resources on the greatest vulnerabilities;
- develop protective action plans to enhance system reliability and public safety;
- design and implement a national dam security program to institutionalize best practices;
- develop emergency action plans to mitigate risks from dam incidents

6. Disruptions to Financial Institutions

- assess risk and vulnerability for a range of financial institutions, including stock exchanges and banking organizations; this list is not exhaustive, but at least gives an overview of problems
- determine consequences and mitigation steps for a variety of disruptions including failures of computer systems and damage to physical facilities

Despite the fact that different sectors have their own specifics there is a need for comprehensive and integrated approach taking into account interdependencies and common methodology, which can be applied.

7. Control Systems

- Principal task is developing best practices and new technologies to strengthen the security of control systems, and identifying the most critical control system sites and developing a prioritized plan for ensuring cyber security at those sites, including:
- guidelines for development of a comprehensive and coordinated national plan , which delineate the roles and responsibilities of all entities, define interim objectives and milestones, set time frames for achieving objectives, and establish performance measures;
- guidelines for development and implementation of effective security management programs of entities, including their policies that consider control system security;
- development and outreach of guidance and methodologies for vulnerability assessment of control systems;
- assess vulnerabilities to cyber attacks related to connection to other networks, insecure connections or resulting from public availability of information about infrastructures and control systems;
- ensure that there is broad awareness of the vulnerabilities in control systems and the consequences of exploiting these vulnerabilities

Conclusions

We have attempted to prepare a list of the most important tasks for critical infrastructure protection, which should be accomplished in a short period in different sectors. We have reviewed a number of articles and materials available on the Web for this collection. It should be clear that this list is not exhaustive, but at least an overview is given about problems, that should be solved. Despite the fact that different sectors have their own specifications, there is a need for comprehensive and integrated approach taking into account interdependencies and common methodologies. We think that the presented list of tasks will stand the basis for critical infrastructure security analysis also in Poland.

Middleware for a dependable info'structure in energy applications

Middleware architecture yields transparency and dependability to control applications for dispersed electricity generation.

Geert Deconinck

Prof. Dr. ir. G. Deconinck
K.U.Leuven
Electrical Engineering Dept (ESAT)
ELECTA
Kasteelpark Arenberg 10
B-3001 Leuven
Belgium
Geert.Deconinck@esat.kuleuven.be

Several experts at the recent European workshop on "The future of ICT for power systems: emerging security challenges" [8] agreed that the current communication and control system that underpins the electric power systems did not change significantly over the last 40 years. Yes, SCADA systems became more performing and computation power has increased significantly, but control remains largely centralised and several control loops contain human interference communicating via telephone, fax and email [6]. Even more, humans can only interpret/process a limited amount of information, as a result of which more than 95 % of the captured data is dissolved in the aggregation process. Hence, autonomous decentralised systems provide a tremendous opportunity to improve monitoring and control operations, optimising the overall electric power system. This opportunity will become even more attractive as ever more intelligent electronic devices (IED) are being deployed, while new measurement devices, such as synchronous phasor measurement units (PMUs), gather data several times in each power cycle.

As a target electrical energy application, we consider dispersed generation, where different small-scale renewable energy resources (wind, photovoltaic, combined heat/power) provide partial coverage of the electricity needs at distribution level.

There are many problems involved in designing a well-suited *info'structure* (information infrastructure) that can serve in an environment of decentralised electrical energy applications.

- Communication architecture: Which communication architecture is appropriate to support point-to-point communication as well as broadcasting and multicasting of information? Indeed, for different purposes, a component needs to exchange information with different other components (e.g. for protection purposes, for stability control, for economic optimisation of set points, etc.). Which models for information exchange need to be supported (push/pull, event-triggered/time-triggered, …) ?
- Interoperability: System operators are required (by economic reasons) to switch from dedicated communication systems from a single vendor towards interoperable, multivendor protocols, implying that all equipment must be able to communicate with off-the-shelf equipment from other vendors, or from peer system operators. Several communication protocols are being proposed as more generic solutions (e.g. IEC61850, CA2.0, TASE.2 (ICCP), DNP3, IEC 60870-5-10x, OPC, …). These many standardisation initiatives also show that industry itself feels the urgent need for a solution, which is not there yet. However, the multitude of solutions proves that consensus

needs further rounds of discussion and study.

- Dynamic aspects and different timescales: Due to switching of generators and loads, the components that need to communicate will vary in time, and hence, the logical communication topology has to follow accordingly. Furthermore, some phenomena require a control action within a few cycles, while others have seconds or even minutes of reaction time. In current situations, some local control algorithms require no communication, while the centralised approaches require several roundtrip transmission periods; hence, they make use of dedicated (expensive) communication lines if the communication latency of the centralised approach is not sufficiently short (e.g. for SPS - special protection systems- and WAMS -wide area measurement systems-).
- Dependability aspects: Which aspects influence the dependability of the communication and how does this affect the control functions that rely on it. What are relevant fault and failure models? Which quantitative levels of availability, error detection latency, etc. are required? How can messages be timely delivered on top of an unreliable communication infrastructure? It is insufficient to just plug in a communication network in order to be successful, but rather there needs to be a communication architecture that is flexibly, predictable, scalable, reliable and provides information security (integrity, confidentiality, authentication, availability), and different quality-of-service levels.

All these requirements call for appropriate middleware to manage communication and mechanisms to integrate fault tolerance. As such, the *information infrastructure –off-the-shelf* ICT equipment (HW, network, system SW and application SW) that is used for communication and control – needs to deal autonomously with this dynamic environment and varying network topologies [1], [2], [3], [4], 0.

2. Middleware Architecture

We are designing a middleware architecture (between the application software and the operating system) that autonomously determines neighbors of a component in this dispersed generation environment, and establishes communication links among them. It is based on a resource discovery algorithm in a peer-to-peer network [13]. An XML description of functionality allows to logically group entities with similar functionality together (meters, manageable loads and generators, etc.). As such, a hierarchical structure is created for data and information aggregation and for distributed cooperation and control among the entities.

If the communication topology modifies, this needs to be transparent to the electricity application.

This communication infrastructure periodically checks for modifications: entities or links may appear, disappear or re-appear due to functional behaviour (no wind), due to electrical faults (short-circuits), or due to physical faults in the ICT infrastructure (controller or network breakdown). Indeed as parameters and functionality of entities can change dynamically, so does the XML description; hence, the information infrastructure needs to be adapted accordingly.

It is supported by flexible software modules at middleware level, one for each device connected to the network, which periodically scan their environment and put up/break or modify the connections. This provides a network abstraction to the applications allowing them to communicate based on their functionality (i.e. logical architecture), rather than on the physical topology of the network.

Data traffic can be separated into a vertical and a horizontal data stream. The former, e.g. between substations and meters, is composed of a data stream *spreading* downwards, e.g. distribution of policies and control objectives, and a data stream *aggregating* upwards, e.g. collection and processing of measured electrical data. The horizontal data streams (between similar units such as substations or between meters) are composed of distributed control and bookkeeping data to create a dependable logical topology. For instance, fault tolerance mechanisms can be integrated, because neighbouring similar entities collect overlapping information, which can be used to detect measurement errors or to mask faults in the information infrastructure.

Case study

This information infrastructure is currently being deployed in several case studies, in order to quantitatively evaluate performance and dependability characteristics: For instance, it is used to interconnect and control a*ctive filters*, integrated in power electronic converters coupled to generation units for renewable energy. With these devices, the Power Quality can be enhanced as the active power production for some sources of renewable energy (e.g. windmills) is rarely at its maximum and, consequently, a considerable amount of non-active power is available for power quality unbalance compensation during such periods [7], [8]. Therefore, power quality parameters are measured on several positions in the electrical grid, and forwarded over the information infrastructure to the other converters.

At the research group’s laboratory, a testbed is being developed which

Figure: Practical setup of Herakles platform with 3 power electronic converters, interconnected via a TCP/IP based info'structure.

integrates the electric power system and the information infrastructure. It consists of several power electronic converters, which are interconnected via off-the-shelf communication protocols (TCP/IP). It is based on the Herakles platform [8], developed at K.U.Leuven. Each converter can be used to emulate generators or loads in a dispersed electricity generation environment.

This Herakles platform allows different control ideas (voltage/frequency/current control, power quality control, etc.) to be modelled in a high level programming tool such as Matlab, after which it can be swiftly prototyped on a 4-quadrant power electronic converter, whereby the control algorithms are downloaded on high performance signal processing hardware (DSP + FPGA) which manages the power electronics. This DSP is connected to a PC which allows communication with other intelligent components over TCP/IP in order to implement local, hierarchical and decentralised control algorithms. (See figure.)

With this setup, the integrated middleware is able to provide a robust control solution within a dynamic environment.

References

[1] M. Adamiak, W. Premerlani, "Data communications in a deregulated environment," *IEEE Computer Applications in Power*, 12(3):36-39, Jul. 1999.

[2] M. Amin, "Towards self-healing energy infrastructure systems," *IEEE Computer Applications in Power*, 14(1):20-28, Jan. 2001.

[3] A. Bose, "Power System Stability: New Opportunities for Control," Chapter in "Stability and Control of Dynamical Systems and Applications," D. Liu, P.J. Antsaklis (Eds), Birkhäuser (Boston), 2003.

[4] G. Deconinck, V. De Florio, O. Botti, "Software-Implemented Fault-Tolerance and Separate Recovery Strategies Enhance Maintainability," *IEEE Trans. Reliability*, Vol. 51, No. 2, Jun. 2002, pp. 158-165.

[5] A. Dusa, G. Deconinck, R. Belmans, "Communication in Intelligent Residential Electrical Installations," *Proc. IEEE Young Researchers Symp. in Electrical Power Engineering*, Delft, The Netherlands, Mar. 2004, 5 pages.

[6] C.H. Hauser, D.E. Bakken, A. Bose, "A Failure to Communicate," IEEE Power & Energy Magazine, Vol. 3, No. 2, Mar. 2005, pp. 47-55.

[7] G. Joós, B.-T. Ooi, e.a., "The potential of distributed generation to provide ancillary services," *Proc. IEEE Power Eng. Soc. Summer Meeting*, 2000, pp. 1762-1767.

[8] K. Macken, K. Vanthournout, e.a., "Distributed control of renewable generation units with integrated active filter", *Proc. IEEE Power Electronics Specialists Conf.*, Vol. 2, Acapulco, Mexico, Jun. 2003, pp. 741-747.

[9] A. Stefanini, A. Servida, Joint DG INFSO, DG RTD and JRC workshop on R&D challenges: The future of ICT for power systems: emerging security challenges, Brussels, Belgium, 3-4 Feb. 2005.

[10] J. Van den Keybus, B. Bolsens, K. De Brabandere, J. Driesen, "Using a fully digital rapid prototype platform in grid-coupled power electronics applications**,**" 9th IEEE Conference on Computers and Power Electronics (COMPEL 2004), Champaign-Urbana, USA, August 15-18, 2004; 10 pages.

[11] K. Vanthournout, K. De Brabandere, E. Haesen, J. Van den Keybus, G. Deconinck, R. Belmans, "Agora: Distributed Tertiary Control of Distributed Resources," accepted for *Proc. of 5th Power Systems Computation Conf. (PSCC-2005),* Liège, Belgium, Aug. 2005.

[12] K. Vanthournout, G. Deconinck, R. Belmans, "A Middleware Control Layer for Distributed Generation Systems," *Proc. of IEEE Power Systems Conference and Exhibition (PSCE-2004),* New York City, NY, Oct. 10-13, 2004, 5 pages on CDROM.

[13] K. Vanthournout, G. Deconinck, R. Belmans, "Building Dependable Peer-to-Peer systems", *Proc. 3rd Workshop on Architecturing Dependable Systems* (organised with DSN-2004), Florence, Italy, Jun. 2004.

Towards a global security and dependability framework

The CyberDefense Project is an international initiative that addresses the protection of critical IT and telecommunication infrastructures against malicious threats such as worms, denial-of-service attacks, spyware and spam.

Engin Kirda and Christopher Kruegel

Engin Kirda is currently an assistant professor with the Distributed Systems Group at the Technical University Vienna. Engin Kirda received his Ph.D. in computer science from the Technical University Vienna. He can be reached at engin@infosys.tuwien.ac.at.

Christopher Kruegel is currently an assistant professor with the Automation Systems Group at the Technical University Vienna. Before that, he was working as a research post-doc for the Reliable Software Group at the University of California, Santa Barbara. Christopher Kruegel received his Ph.D. in computer science from the Technical University Vienna. He can be reached at chris@auto.tuwien.ac.at.

Computer networks, and in particular the Internet, play a fundamental role in our society by providing the technological basis for a large number of applications ranging from e-Commerce to e-Government. The member states of the European Union recognized the need to make further progress to keep the development of the e-Economy as a priority on the European policy agenda (see for example the eEurope initiative, launched at the European Council in June 2002, aiming at developing modern public services and a dynamic environment for e-Business). Also, it is anticipated that the role of computer networks will increase tremendously over the next few years, as smart phones and IP-based mobile devices are deployed at a large scale.

About 1,700 new malicious programs (such as computer viruses, Trojan horses or worms) are discovered every month

Increasing number of attacks

Attacks against computer networks pose an enormous threat to digital infrastructures that underpin e-Europe, resulting both in economic losses and privacy problems. The number of reported security incidents has increased almost exponentially over the past few years and it is realistic to assume that this trend will continue in the near future. For example, about 1,700 new malicious programs (such as computer viruses, Trojan horses or worms) are discovered every month – this amounts to almost 55 new security threats per day!

Protecting critical IT and telecommunication infrastructures against malicious threats (such as worms, denial-of-service attacks, spyware and spam) is thus of strategic importance both for the European economy and society. Without availability of effective security measures that protect critical European network infrastructures, the vision of e-Europe is likely to fail.

Europe is lagging behind

While various research activities on cryptographic foundations and implementations of secure IT systems have been performed at the European level (involving both EU-IST Network of Excellences and Specific Targeted Research Projects), much less European effort is put in research activities related to secure computer and telecommunication networks. A significant part of network security research is still performed outside Europe, most importantly in the US. In this respect, the US National Science Foundation recently funded a Centre for Internet Epidemiology and Defences, to be established by the University of California at San Diego and the International Computer Science Institute affiliated with the University of

California at Berkeley. With $6.2 million in funding over five years, the centre will develop technologies to detect, analyse and defend against large-scale Internet attacks.

Europe clearly suffers from a lack of expertise in the area of critical computer network infrastructure security. As a consequence, opportunities to establish European companies as key players in the field and to make the European Information Society more dependable and secure are missed. More effort is required to assure that European researchers take a leading role in the upcoming years.

Cyberdefense

The CyberDefense Project is an international initiative that addresses the protection of critical IT and telecommunication infrastructures against threats such as worms, denial-of-service attacks, spyware and spam. The project partners include large companies such as France Télécom, small enterprises such as Ikarus Software (an anti-virus vendor), and European universities such as the Technical University Vienna.

CyberDefence will provide mechanisms that enable to construct an effective system for preventing malicious attacks against critical IP-based networks that are composed of different, interconnected heterogeneous components.

Europe clearly suffers from a lack of expertise in the area of critical computer network infrastructure security

The project follows an interdisciplinary approach, linking traditional concepts of computer security with methods of formal analysis that are successfully applied in other branches of computer security research. This approach is promising to provide more accurate and reliable network protection routines that can adapt to newly emerged security threats. In addition, the adoption of the project results on a large scale has economic advantages compared with traditional network protection mechanisms.

Within CyberDefence, special emphasis is put on the participation of small and medium-sized enterprises (SMEs), both as suppliers and users of knowledge and technologies. The reason is that SMEs are key project partners that enable quick transfer of knowledge to business assets and products.

An essential factor for the success of computer network security research is the ability to model real security incidents in a synthetic and controlled environment. Through modelling and simulation, one can obtain a clear understanding of the impact and consequences of an attack and its appearance at different network components (such as gateways or firewalls). This information enables the construction of effective countermeasures particularly tailored towards specific network components and threat classes. In addition, a thorough understanding of the timing conditions of an attack is necessary to assure a timely deployment of countermeasures.

Within CyberDefence, modelling and simulation is performed at two stages. First, modelling methods are used to obtain a thorough understanding of the impact of an attack on the protected network and the appearance of the attack at different network components. Second, methods of simulation are used to evaluate the impact of the proposed cyber defence system on the protected network. An integral part of the research performed within CyberDefence will thus be devoted to modelling and simulation aspects of network security incidents. We expect that CyberDefence will advance scientific knowledge in the field of network security incident modelling. In addition, the practical research work performed within the project will result in a range of readily available modelling and monitoring tools.

While network forensics is not a core topic of the project, the methodology developed within CyberDefence enhances the capabilities to timely react against network security threats, in particular against malicious programs. Complementary to technical protection mechanisms, coordinated emergency plans are the key elements to combat IT security attacks. However, realistic emergency plans can only be engineered upon a profound knowledge of possible attack scenarios, as generated within this project.

CyberDefence will therefore liaise with national Computer Emergency Response teams (CERTs) as well as national computer security organizations in order to incorporate the knowledge on malicious programs created within this project into their emergency plans. Two CyberDefence partners (Ikarus Software and the Technical University Vienna) are already active members of the CIRCA (Computer Incidence Response Coordination Austria) project, established by the association of Austrian Internet Service Providers (ISPA). The main goal of CIRCA is to prevent local or global attacks on the core Austrian Internet backbone, and to build an infrastructure to regain functionality after partial or global breakdowns. This goal is achieved by coordinating the efforts of security officers from both private and public bodies. CyberDefence will actively participate in CIRCA, providing both the knowledge generated within the project and the prototype implementation of the cyber defence system.

Concluding Remarks

Current security solutions address the problem of securing a particular protection domain. Perimeter security devices (e.g., firewalls) and secure communication environments such as virtual private networks (VPNs) are deployed to keep unwanted traffic out of the internal network. In addition, malware detection systems such as virus scanners and intrusion detection systems (IDS) are used. These systems analyse information about the activities performed in computer systems and networks, looking for signs of known malicious code or malicious behaviour.

Unfortunately, security solutions that are currently available cannot adequately address existing threats. One problem is that only known attacks can be identified. The reason is that an appropriate signature must be provided to a sensor before the corresponding attack can be detected. Thus, a window of vulnerability exists between the time an attack (or a virus, worm) is seen for the first time, and the time the signature is installed.

A long window of vulnerability is particularly problematic when dealing with aggressive and fast-spreading computer worms such as CodeRed or Slammer. The reason is that it is necessary to detect a worm in the early stage of its spread to be able to successfully deploy defence mechanisms on time. Otherwise, if the worm reaches a stage of exponential growth, even effective countermeasures cannot deal with the sheer volume of malicious worm traffic that is generated. Therefore, **local surveillance** mechanisms have to be developed that can *identify novel attacks*.

Also, for large-scale cyber threats, local surveillance is not sufficient. Recent worm epidemics and distributed denial-of-service attacks have demonstrated that future threats will typically involve numerous protection domains as victims or unwilling collaborators.

Therefore, there is a need to create a global security infrastructure that enables the correlation of security-related information from different subsystems to obtain an overview of the security state of the complete infrastructure as a whole. This has to be combined with a central control station that disposes of the necessary command and control capabilities to react to emerging threats and initiate coordinated countermeasures in a reliable and robust way. In the event of an emerging worm, the ability to combine information coming from different parts of the network and to coordinate countermeasures is vital. Therefore, local surveillance must be complemented by a **global coordination and control** infrastructure to *detect and respond to coordinated attacks as well as worm and virus activity*.

In the CyberDefence project, we aim to address the issues outlined above and implement a global coordination and control cyber defence system for critical large-scale IP networks.

Assessing Software Safety and Security for Critical Infrastructures

As for critical infrastructures the interaction of safety and security issues becomes growingly complex, licensors cannot further rely on the classical principle of separation of concerns, as might have been practicable until recently. Today, standards are required in order to assess the overall system trustworthiness.

Francesca Saglietti

Professor and Head of Department of Software Engineering
University of Erlangen-Nürnberg
Germany

saglietti@informatik.uni-erlangen.de
www11.informatik.uni-erlangen.de

In general, complex software-based systems cannot be assumed to be perfectly designed or implemented; they will rather contain vulnerabilities, which may lead under certain circumstances to undesired events with critical consequences due to loss of values, such as

- ***existential*** values (e.g. human life, human health, environmental balance),

- ***material*** goods (e.g. financial assets, material infrastructures, valuables),

- ***business*** values (e.g. time, service performance, user comfort),

- ***ideal*** values (e.g. privacy, information).

Obviously, any kind of loss indirectly also induces a damage in terms of ***reputation***.

A ***threat*** is a class of events, which may give rise to critical consequences, if inherent vulnerabilities allow such events to propagate to dangerous system misbehaviour. Threats may relate to

- ***intentional*** attacks, but also to

- ***organisational*** deficiencies,

- ***human*** mistakes,

- ***technical*** casualties,

- "***force majeure***".

An ***incident*** is an instance of a threat, i. e. a specific threat scenario in the presence of a vulnerability allowing critical short-term or long-term consequences.

A unified licensing approach is required to assess trustworthiness w.r.t. safety and security

On the basis of this terminology, ***trustworthiness*** may be taken to mean freedom of incidents (even assuming the existence of sporadic threats).

Historical Development

Safety. As long as computers involving a certain degree of risk operated in a closed environment (typically embedded software-based systems supporting the automatic control of transportation systems or industrial plants) the only term safety was sufficient in order to address software trustworthiness with respect to the absence of danger by computer misbehaviour (especially for persons and material infrastructures potentially affected).

Security. As soon as systems got increasingly networked to exchange information, another source of threats came up, namely misuse of data to be processed by a communication network. Typically, such misbehaviour consists in accessing information, manipulating data, or sending messages in such a way as to endanger system performance or privacy.

This was the time when the term security came in use to address trustworthiness with respect to the absence of danger by computer misuse (especially for information and services potentially affected).

Critical Information Infrastructures. Nowadays, large networked systems are responsible for safety-related tasks, their communication network, for its part, being subject to security threats. The combination of both threat types leads to the necessity of considering potential interactions of unsafe and insecure system properties. Typical examples are:

- storage of patient data which, if subject to manipulation, may lead to the application of inadequate medical or technical therapy;

- computer-controlled transportation systems making use of data transmission, e.g. radio-controlled train speed control, remote-controlled car maintenance, vehicles communicating as autonomous agents.

Depending on the overall goal to be achieved by the application envisaged, different causal relations between safety and security may be of interest:

- ***security implications on safety***: security vulnerabilities may contribute to safety incidents, for example, in case of attacks to data integrity leading to vital computer failures;

- ***safety implications on security***: safety vulnerabilities may contribute to security incidents, for example, in case of logical (or physical) faults in the design of a complex access control system leading, via safety incidents, to security breaches.

Differences

Intentionality of Threats. The classical parameter chosen to distinguish between safety and security concerns the underlying intentionality of the threat:

- usage of the term ***safety*** usually assumes the absence of incidents due to unintentional faults (of logical or physical nature), while

- in general the term ***security*** is taken to represent the absence of incidents due to intentional attacks.

In this article, this view is not taken. The attitude recommended here is to guide the engineering approach by effect-driven rather than cause-driven considerations. The fault-handling mechanisms to be effectively applied relate to the consequences of threats and vulnerabilities rather than to their intentional background, whose human nature may not be observable, nor provable.

Values to be Protected. A more informative parameter may be taken to discriminate between safety and security incidents, namely the classes of values affected by an incident:

- ***security*** is characterized by absence of (or at least limited occurrence of) incidents causing damage to ideal or business values, in particular incidents involving undesirable consequences to data, information or service performance of a computer system;

- ***safety*** is characterized by absence of (or at least limited occurrence of) incidents severely affecting existential and / or material values in the environment of the computer system, in particular endangering life and limb, environmental balance or material structures.

It may be argued that the distinction between ideal, business and material values may involve some ambiguity. Nonetheless, for the purpose of classifying safety resp. security demands it is felt to be of essential importance to characterize qualitatively and quantitatively different loss types which might result from uncontrolled incidents.

Risk (threat) = Probability of occurrence (incident) ∗ Amount of loss (incident)

Vulnerabilities and Threats to be Controlled. In terms of identifying an adequate development and licensing process, in accordance with the (safety resp. security) risks involved by the application envisaged, a thorough system analysis should take into account (beyond the criticality of potential loss) also the location of vulnerabilities and threats, distinguishing between

- ***safety*** mechanisms aiming at protecting the computer environment (including users as well as other human beings and natural entities placed in a computer-controlled geographical area) from misbehaviour of the computer itself (typically due to logical flaws, or to physical effects like aging, wear-out, radiation, etc.) and

- ***security*** mechanisms aiming at protecting the computer itself (including data, information and service performance) from misbehaviour of the computer environment (due to inexpert usage or, more typically, by intentional criminal attacks).

Risk Analysis. In order to evaluate the degree of criticality potentially involved by a computer application and to scale the demands on the rigor of its development and licensing procedures accordingly, it is necessary to estimate the underlying risk by taking into account the following aspects:

- the elements (objects, functions, data, human beings), which may be threatened, as well as

- for each threat identified, an estimation of the probability of incident occurrence and of the amount of loss to be expected.

For each potential threat identified, its criticality may be quantitatively estimated in terms of the threat-specific risk by means of the product of the probability of incident occurrence and of the amount of loss to be expected from such incidents.

Standards

An important question concerns the rationale to be followed in order to define appropriate process criteria permitting to achieve given quality demands. In the following, a number of existing standards and of documents in preparation are addressed, which base their recommendations on a hierarchy of demands. While most of them address either safety or security issues, a unified licensing procedure is still the target of ongoing work.

Safety Standards. Common to all approaches presented, although at different level of detail, is a preliminary risk analysis aimed at classifying the criticality of incorrect software behaviour. According to the resulting safety classification, the major standards provide corresponding levels of quality required to be demonstrated for the purpose of licensing.

Generic Standard. The safety classification underlying the generic standard [IEC 61508] is based on the probabilistic quantification of minimum software reliability demands determined by comparing the hazards involved by software-based automation with those inherent to the technical application considered. Such a risk analysis yields ***Safety Integrity Levels (SILs),*** as shown in table 1, distinguishing between discrete and continuous operation modes.

Software for Automotive Systems. A further safety classification of deterministic nature was developed for the British automotive industry (s. [MISRA 94]). In view of the human-controlled driving process, this approach takes into account the driver's chances to control unexpected software failures during operation.

This view of human-machine interaction results in the categories shown in table 3 and corresponding quality demands.

Safety Integrity Level	average probability of failure on demand	probability of failure per hour
4	$10^{-5} \le x < 10^{-4}$	$10^{-9} \le x < 10^{-8}$
3	$10^{-4} \le x < 10^{-3}$	$10^{-8} \le x < 10^{-7}$
2	$10^{-3} \le x < 10^{-2}$	$10^{-7} \le x < 10^{-6}$
1	$10^{-2} \le x < 10^{-1}$	$10^{-6} \le x < 10^{-5}$

Table 1: Safety classification according to **IEC 61508**

This standard has the merit of offering a generic framework permitting to be adapted to different application areas. On the basis of the SIL identified, the standard defines demands on product and process properties.

Software for Medical Devices. In order to avoid the problematic determination of probabilistic figures, alternative standard approaches propose to scale safety demands according to worst-case scenarios. This applies for example to the licensing of software for medical devices (s. [IEC 62304]), as shown in the following table 2.

Further Application Areas. Similar approaches, except for application-specific differences, are taken for software-based control systems in the following industrial areas:

- process industry
  (s. [IEC 61511]),
- nuclear industry
  (s. [IEC 61226] and [IEC 62138]),
- machinery
  (s. [IEC 62061]),
- railway systems
  (s. [EN 50128]).

Class A	***No injury*** may occur to the patient or to the operator resulting from a hazard to which the software item may be a contributing factor
Class B	***Non-serious injury*** may occur to the patient or to the operator resulting from a hazard to which the software item may be a contributing factor
Class C	***Death or serious injury*** may occur to the patient or to the operator resulting from a hazard to which the software item may be a contributing factor

Table 2: Safety classification according to **IEC 62304**

Security Standards. The ***Evaluation Assurance Levels (EALs)*** proposed by the well-known Common Criteria for Information Technology Security Evaluation(s. [CC 99]) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance:

- EAL1: functionally tested,
- EAL2: structurally tested,
- EAL3: methodically tested and checked,
- EAL4: methodically designed, tested, and reviewed,
- EAL5: semiformally designed and tested,
- EAL6: semiformally verified design and tested,
- EAL7: formally verified design and tested.

When compared with the above-mentioned safety standards, the hierarchy underlying the Evaluation Assurance Levels is primarily characterized by increasing degrees of rigor demands on functionality, design, verification and test. In this sense, the classification is process-related, rather than effect-related. The question left open here is how to identify the appropriate Evaluation Assurance Level in a systematic, reproducible way. While in some cases the identification of a suitable EAL may be carried out in an intuitive way, this procedure may become unacceptably complex for large critical infrastructures.

Unified Approaches for Critical Infrastructures. The question of defining appropriate security demands for safety-related systems is addressed in a new IEC proposal titled "Security for Industrial Process Measurement and Control", which suggests to carry out a qualitative analysis of

- factors influencing the **likelihood of occurrence** of an attack, as well as of
- factors influencing the **severity of consequences** of an attack.

and to identify for each of them an acceptable security level. The maximum level over all factors is then taken to determine the overall ***Security Requirements Level (SRL).***

Categories	Definition	SIL
Uncontrollable	This relates to failures whose effects are ***not controllable*** by the vehicle occupants, and which are most likely to lead to extremely severe outcomes. The outcome cannot be influenced by a human response.	4
Difficult to control	This relates to failures whose effects are ***not normally controllable*** by the vehicle occupants but could, under favourable circumstances, be influenced by a mature human response. They are likely to lead to very severe outcomes.	3
Debilitating	This relates to failures whose effects are ***usually controllable*** by a sensible human response and, whilst there is a reduction in the safety margin, can usually be expected to lead to outcomes which are at worst severe.	2
Distracting	This relates to failures which produce ***operational limitations***, but a normal human response will limit the outcome to no worse than minor.	1
Nuisance only	This relates to failures where ***safety is not normally considered to be affected***, and where customer satisfaction is the main consideration.	0

Table 3: Safety Classification according to **MISRA**

In other words, the above-mentioned quantitative risk evaluation is here replaced by a more simplistic view, whose accuracy may be questionable. On the other hand, this approach has the merit of addressing for the first time the problem of analyzing security demands for industrial automatic control systems.

Fault Tree Analysis. From a scientific point of view, a more accurate analysis technique would make use of fault trees:

- For each class of safety threat identified, sub-events responsible for its occurrence are derived top-down; they may include security incidents.

- Successively, the minimal cut sets of the fault-tree are determined.

- Finally, depending on the criticality of the top event (in terms of the amount and type of loss expected) and on the size of minimal cut sets containing a given security incident, demands on protection against it are systematically derived.

Conclusion

This article briefly summarizes classical differences and historical trends in analyzing safety and security demands.

After a brief survey on terminology, offering a uniform view to both dependability attributes, the article focuses on a number of normative documents with diverse approaches to determine appropriate safety resp. security demands.

For today's growing critical infrastructures it is felt that this question is becoming increasingly important and should be handled in a unified, systematic way by means of an extended fault tree analysis, capable of integrating security incidents as sub-events possibly leading to safety-related failures.

References

[CC 99] Bundesamt für Sicherheit in der Informationstechnik (BSI). 1999. Common Criteria for Information Technology Security Evaluation, CC 2.1, aligned with International Standard ISO / IEC 15408

[EN 50128] European Committee for Electro-technical Standardization (CENELEC). 2001. Railway Applications: Software for Railway Control and Protection Systems, European Norm

[IEC 61226] International Electro-technical Commission (IEC). 1993. Nuclear Power Plants - Instrumentation and Control Systems Important for Safety - Classification. International Standard

[IEC 61508] International Electro-technical Commission (IEC). 1998. Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, Part 3: Software Requirements. International Standard

[IEC 61511] International Electro-technical Commission (IEC). 2003 / 2004. Functional Safety: Instrumented Systems for the Process Industry Sectors. International Standard

[IEC 62061] International Electro-technical Commission (IEC). 2004. Safety of Machinery – Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems. Final Draft International Standard

[IEC 62138] International Electro-technical Commission (IEC). 2004. Nuclear Power Plants - Instrumentation and Control important for Safety - Software aspects for computer-based systems performing category B or C functions. International Standard

[IEC 62304] International Electro-technical Commission (IEC). 2004. Medical Device Software - Software Life-cycle Processes. Committee Draft

[IEC 2005] International Electro-technical Commission (IEC). 2005. Security for Industrial Process Measurement and Control - Network and System Security. New Work Item Proposal

[IEV 01] Internationales Elektrotechnisches Wörterbuch. 2001. Beuth Verlag

[LAP 92] J.-C. Laprie. 1992. Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese. Springer-Verlag

[MISRA 94] Motor Industry Software Reliability Association. 1994. Development Guidelines for Vehicle-Based Software

Special Interest Group KRITIS formed at German Informatics Society.

Most working groups dealing with critical information infrastructure protection have to follow a closed shop' strategy. At German Informatics Society (GI) the special Interest group KRITIS formed an open platform for discussion, exchanging information and helping CIIP ‚going public' on a reliable foundation.

Dirk Schadt

Chair of GI-KRITIS and Business Technologist Security Strategy at Computer Associates

How to deal with serious threats in our world is being analyzed and discussed in a lot of working groups with CIP, CIIP or ‚homeland security' in their name and goal definition. All of them are interest groups of some kind and follow more or less a closed shop strategy. The goal of GI KRITIS is to supply an open platform for everybody to enable awareness in the public and supply room for discussion on how to really solve challenges of vital environments.

Regulations still demand ineffective countermeasures

Former efforts on analyses and studies of the main domains of critical infrastructures did not help the pertained parties to know the countermeasures on how to effectively mitigate risks in the case of disaster and provide continuity. Most of the guidelines and regulations to prepare better on disaster recovery tend to a technical approach supplying more high availability and install more technology.

Independence and neutrality seem to be the key success factors to force awareness and enable public discussion.

Pertained parties are not involved enough

Learning's from real cases in the past should lead to think also about methodology of crisis management, sharing responsibilities, communication with pertained parties and the public, practical preparation and training. These things happen but often partly and seldom are all pertained parties included and often in closed groups without information on success.

Therefore a very natural and logical step was to form an independent and neutral platform for open discussion and invite all parties. As we, the founders, have strong links to the German Informatics Society (GI) and got the chance to form the specila interestt group KRITIS within the competence group SECURITY.

Building awareness and trust needs competency

That way we believe we have an optimal start for even bringing hardened frontiers back to discussion because politics and lobbyism are not tuned instruments for a wide open forum and discussion. Competency is a factor to build awareness and trust between all members.

Obviously CIP covers more than informatics. We both, GI and KRITIS, are aware that areas of engineering and internationality are not fully covered by the organization of GI. But e.g. to fulfil inter communication concepts informatics is needed, and areas of safety and reliability are not limited to production only.

With the help of scientists, operations of pertained infrastructures, the German government and well known experts we are proud to be announcing the 2nd. Symposium‚CIP Europe 2005' attached to the annual GI convention on 19th September 2005 in Bonn.

For further information please visit our German websites: http://www.gi-fb-sicherheit.de/fg/kritis/

First IEEE International Workshop on Critical Infrastructure Protection

November 3 and 4, 2005, at Fraunhofer Institute Darmstadt, Germany
An international workshop on C(I)IP will be held, with speakers from research and practitioners from across the globe.

Stephen D. Wolthusen

Associate professor at the Norwegian Information Security Lab, Gjøvik University College and senior scientist at Fraunhofer-IGD, Darmstadt, Germany

The first IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005) is sponsored by the Institute of Electrical and Electronics Engineers (IEEE) Task Force on Information Assurance and is held in cooperation with the Special Interest Group on Critical Infrastructure Protection (FG KRITIS) of the German Gesellschaft für Informatik.

Broad International Participation

The workshop benefits from peer-reviewed talks from a truly international roster of speakers with academic, government, and industry speakers from Brazil, Finland, Israel, Italy, Germany, the Netherlands, Switzerland, and the US. This, together with the spectrum of the talks that cover both technical and organizational or policy-level aspects will ensure that the workshop will provide an important synopsis of the current state of the art and research in the field.

The spectrum of talks will range from technical to policy-level presentations and will provide a timely synopsis of research and ongoing developments in the C(I)IP field

Improved Visibility for C(I)IP

The interdisciplinary character of the C(I)IP challenge is well reflected in the IEEE itself, which with its more than 365´000 members is not only home to the Computer Society but also has 38 societies ranging from aerospace and electronic systems via control systems to nuclear and plasma sciences, many of which are relevant to the C(I)IP mission.

This, together with the fact that IWCIP provides a peer-reviewed outlet for research results, should provide additional impetus for researchers and practitioners to present their findings to a broad, international audience whose dissemination is much wider than that of most CIP events.

An international program committee of renowned area experts has ensured the quality and timeliness of contributions.

By stressing the interactive aspects of the workshop, the organizers hope to foster an atmosphere of frank debate in which these important and occasionally controversial topics can be discussed and future collaborations and cooperation’s can be established.

C(I)IP requires innovative and often interdisciplinary research as well as close cooperation with infrastructure owners/operators, government, and C(I)IP equipment vendors. Ensuring that research and development but also policy can identify the most relevant and urgent questions and address these together with all stakeholders is one of the primary objectives of this workshop.

We would like to invite all interested stakeholders to participate in this workshop and hope to see you in November. For further information see **`http://www.iwcip.org/2005`**

Selected Links an Events

By the end of November it is planned, that a general link document over all ECN Number will be available on the CIIRCO homepage. Please mail interesting links using the topic ECN link to: **editor@ciip-newsletter.org**

Actual Upcoming CIIP Conferences in Europe

- CIIP Conference German Informatics, September 19, 2005 in Bonn: http://www.informatik2005.de/143.html and click on CIS: Symposium 19. September 2005
- First InternationalWorkshop on Critical Infrastructure Protection IWCIP of the Task Force Information Assurance, November 3&4 2005, Darmstadt: http://www.iwcip.org/2005/
- Applied Security Congress and Exhibition September 21&22, Zurich: www.security-zone.info
- International Workshop on "Complex Network and Infrastructure Protection"(CNIP'06) March 28-29, 2006 - Rome, Italy: ciip.casaccia.enea.it/cnip06
- SECURECOMM 2005 www.securecomm.org
- SAFECOMP 2005 www.hrp.no/safecomp2005
- RAID 2005 - 8th International Symposium on Recent Advances in Intrusion Detection: http://www.conjungi.com/RAID/
- ESORICS - 10th European Symposium on Research in Computer Security: http://esorics05.dti.unimi.it/
- ISSE conference: http://www.eema.org/static/isse/
- IEEE International Symposium on High Assurance System Engineering (HASE) http://www.deeds.informatik.tu-darmstadt.de/HASE05
- RSA conference: http://2005.rsaconference.com/europe

Conference Papers and Periodic E-Reports

- EAPC / PfP International Workshop on CIP: http://www.dfae.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec.html
- CIP Report USA, is published once a month, accessible with a email note or from the home page: http://cipp.gmu.edu/report
- International Journal of Emergency Management (IJEM): http://www.inderscience.com/browse/callpaper.php?callID=257
- International Journal of Critical Infrastructures (IJCIS): http://www.inderscience.com/browse/index.php?journalID=58#board
- International Journal of Information and Computer Security (IJICS): http://www.inderscience.com/browse/index.php?journalID=151#objectives
- International Journal of Security and Networks (IJSN): http://www.inderscience.com/browse/index.php?journalCODE=ijsn
- Journal of Computer Security http://www.iospress.nl/html/0926227x.php:
- http://www.mitre.org/public/jcs/
- Information Management & Computer Security: http://www.emeraldinsight.com/info/journals/imcs/imcs.htm
- Information Security Technical Report: http://www.compseconline.com/publications/prodinf.htm

European CIP Activities

- German national plan for protection of the information infrastructure can be downloaded (available in German only) on: http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2005/08/Nationaler__Plan__zum__Schutz__der__Informationsinfrastrukturen.html :
- study on availability and robustness of electronic communications infrastructures: http://ted.publications.eu.int/official/Exec?DataFlow=result_details.dfl&Template=TED/result_details_curr.xsl&Page=1&StatLang=EN

USA Approach (by Hardo Hase, Hase IT GmbH, Germany, hardo.hase@hase-it.de)

- The National Strategy to Secure Cyberspace http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
- DHS Fact Sheet: National Incident Management System (NIMS) http://www.dhs.gov/dhspublic/interweb/assetlibrary/NIMS-90-web.pdf
- National Critical Infrastructure Protection Research and Development Plan http://www.dhs.gov/dhspublic/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf
- Technical Support Working Group Infrastructure Protection http://www.tswg.gov/tswg/ip/ip_ma.htm
- Technical Support Working Group Supervisory control and data acquisition http://www.tswg.gov/tswg/ip/scada.htm
- The Myths and Facts behind Cybersecurity Risks for Industrial Control Systems http://www.tswg.gov/tswg/ip/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf
- 21 Steps to Improve Cyber Security fo SCADA Networks http://www.tswg.gov/tswg/ip/21_Steps_SCADA.pdf
- Survivability Protecting Your Critical Systems http://www.cert.org/archive/html/protect-critical-systems.html

ENEA
Italian National Agency for New Technologies, Energy and the Environment

THE INTERNATIONAL EMERGENCY MANAGEMENT SOCIETY

International Workshop on “Complex Network and Infrastructure Protection”(CNIP’06)

March 28-29, 2006 - Rome, Italy

Objectives of the Workshop

The CNIP’06 International Workshop is aimed at exploring new challenges posed from Complex Network and Infrastructure Protection and promoting a multi-disciplinary approach within the scientific communities at national, European and trans-European level. Special attention will be paid on new threats, vulnerability and suitable defence strategies to prevent, mitigate and manage the emergencies.

The following types of networks and/or infrastructures are considered:

- physical networks, i.e. electrical power transportation grids, oil and gas transportation grids, water distribution networks, transport/road tunnel systems, health care systems etc.
- cyber-networks, i.e. data transmission (Internet based, tele-control and SCADA networks), public telecom and mobile phone networks, e-banking/finance networks etc.
- managerial/organization networks where human resources play a relevant role, such as teams and end-users that supervise and/or utilise the services delivered by the above said infrastructures.

The objective of the Workshop is to bring together experts, emergency managers, infrastructures specialists and stakeholders, with different cultural and scientific backgrounds, to address and analyse the following aspects of Complex Networks and Infrastructure Protection:

- Proposing methods and tools to analyse and understand new risks and vulnerability.
- Giving practical solutions to reduce and mitigate potential dangerous effects.
- Identifying strategies and tools to support emergency managers during critical events.

Call for papers: Authors are invited to submit papers following the instructions available at the Workshop Web site: http://ciip.casaccia.enea.it/cnip06

Scientific Committee *chaired by Sandro Bologna (ENEA - Italy)*

Verner Andersen (Riso National Laboratory, Denmark)
George Apostolakis (MIT, USA)
Claudio Balducelli (ENEA, Italy)
John Bigham (Queen Mary University of London, UK)
Mike Corcoran (NISCC, UK)
Martin Endig (Fraunhofer Institute, Germany)
Bernhard Hammerli (HTA Lucerne, Switzerland)
Dirk Helbing (Univ. of Dresden, Germany)
Erik Hollnagel (Linköpings Universitet, Sweden)
Wolfgang Kroger (IRGC, Switzerland)
Adrian V. Gheorghe (ETH Zurich, Switzerland)
Gwendal Le Grand (ENST, France)
Eric Luiijf (TNO, The Netherlands)
Ann Miller (Univ. Of Missouri-Rolla, USA)
Michele Minichino (ENEA, Italy)
John L. Mitchiner (Sandia National Laboratoy, USA)
Peter Richmond (Univ. of Dublin, Ireland)
Julio G. Rodriguez (Idaho National Laboratory, USA)
Roberto Setola (Univ. Campus Bio-Medico, Italy)
Alberto Stefanini (JRC-Ispra, Italy)
Simin Nadjm-Tehrani (Linköpings Universitet, Sweden)
Salvatore Tucci (Univ. Tor Vergata, Italy)
Sam Varnado (Sandia National Laboratory, USA)
Jean-Luc Wybo (Ecole des Mines de Paris, France)
Enrico Zio (Politecnico of Milan, Italy)

Organisation Committee *chaired by Susanna Del Bufalo (ENEA)*

Fabiola Falconieri (ENEA)
Anna Maria Fagioli (ENEA)
Anna Maria De Micheli (ENEA)
Giordano Vicoli (ENEA)
Claudio Balducelli (ENEA)

Workshop Chair

Claudio Balducelli (ENEA)

Proceedings and papers publication

Regular Proceedings will be produced and distributed at the Workshop. At the same time the Scientific Committee will support the publication of a selection of the accepted papers in the following two scientific journals of Inderscience Publishers: “Int. Journal of Critical Infrastructures” and “Int. Journal of Emergency Management”.