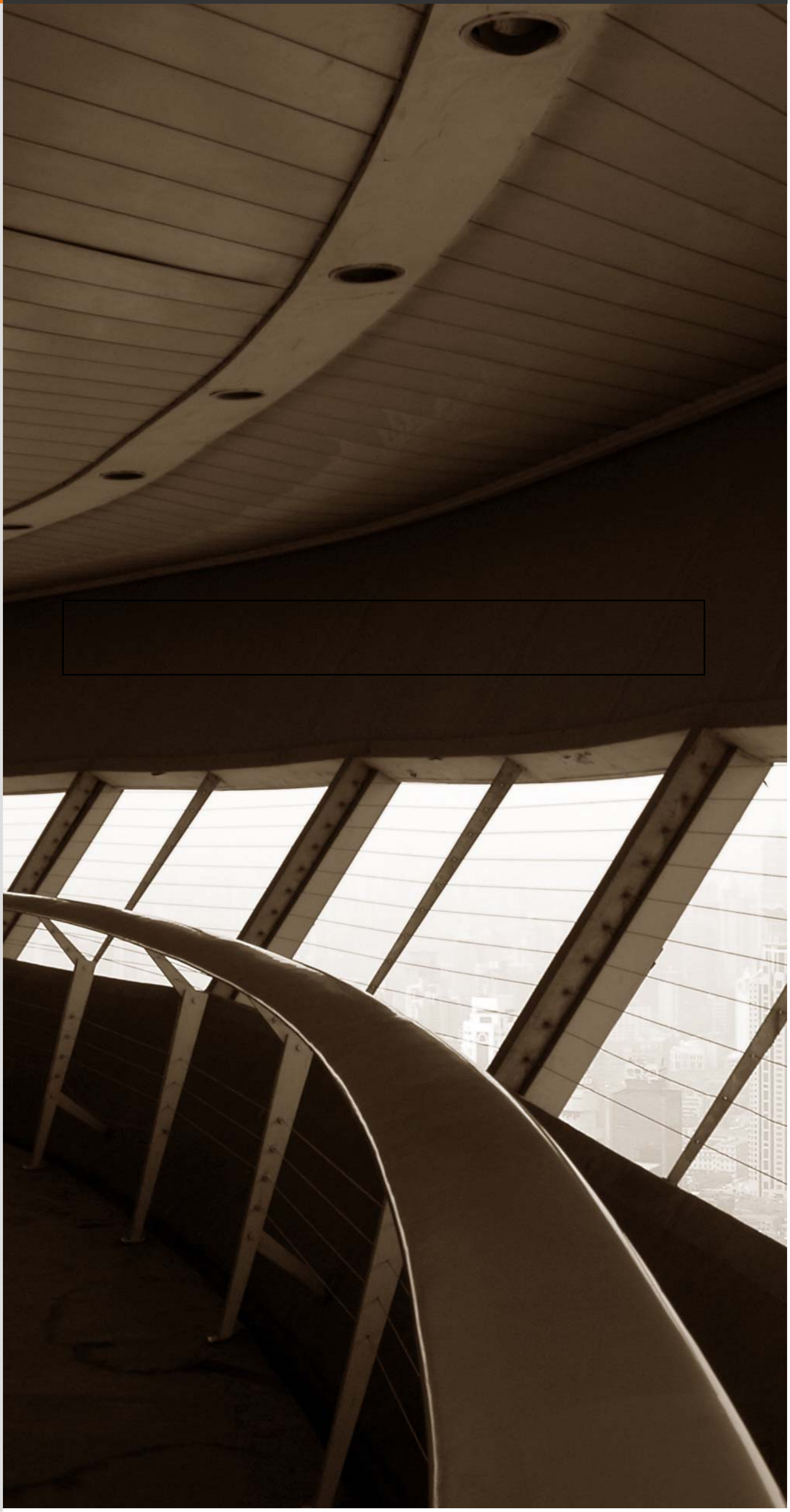
August / September 2009, Volume 5, Number 2

ECN

European CIIP Newsletter



EU research:

- CoMiFin

..-..DIESIS

Supply chain assurance

3rd SCADA Symposium

SCADA security

CFI BCM scenario and cost

CRITIS 2009 Conference: Register now!

> About ECN
ECN is co-ordinated with
The European Commission, was initiated by Dr. Andrea Servida,
and is now coached and supervised by Angelo Marino.
For 2007-2009, the ECN is financed by the IRRIIS project.
The IRRIIS project is an IST FP6 IP,
funded by the European Commission
under contract no 027568

>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 site for specific issues:
http://irriis.org
http://www.ci2rco.org

>Founders and Editors
Eyal Adar CEO iTcon, **eyal@itcon-ltd.com**
Bernhard M. Hämmerli, HTA, Initiator and Main Editor **bmhaemmerli@acris.ch**
Eric Luiijf, TNO Defence, Security and Safety, **eric.luiijf@tno.nl**

>Country specific Editors
For Germany: Heinz Thielmann, Prof. emeritus, **heinz.thielmann@t-online.de**
For Italy: Louisa Franchina, ISCOM, **luisa.franchina@comunicazioni.it**
For France: Michel Riguidel, ENST, **riguidel@enst.fr**
For Spain: Javier Lopez, UMA, **jlm@lcc.uma.es**
*For Finland: Hannu Kari, HUT***, kari@tcs.hut.fi**

> Spelling:
British English is used except for US contributions

Table of Content

Introduction

European Activities

Countery Specific Issues

Method and Models

Method and Models (continued...)

News and Miscellaneous

Selected Links and Events

European R&D and dependencies

The European Commission has started the Coordination Action Parsifal as well as another Specific Targeted Research Project for the critical financial infrastructure (CFI).

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Member of the NICC team.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl

Bernhard M. Hämmerli

Professor in Information Security ISSS
Chair of Scientific and International Affairs
e-mail: bmhaemmerli@acris.ch

It is a well recognised fact that Critical Infrastructures (CI) comprises a set of sectors, with slight differences per nation. There is no debate over the importance of energy, telecommunications, human needs (drinking water, food, and health), transport and financial services. But is there a need to research each sector separately in respect of security and CIP – or is every sector alike?

European R&D has resulted in an increased understanding of CI dependencies. Most CI-sectors understand their critical dependencies and have taken mitigating measures. However, when a specific CI relies on these measures of other CI sectors for their service continuity, failure is the likely outcome because the business continuity planning neglected the second and third level dependencies, e.g. the dependency on fuel for backup generators or the need for specific knowledge in the head of an unavailable person. A second article in a series on business continuity touches some of these aspects.

About this issue

Two European funded research projects, COMIFIN – a middleware for critical financial industry – and DIESIS - .the designing of a federated multipart research facility for CIP are presented first.

An Overview on Software Supply Chain Integrity and its best practice is meant to increase the confidence of all parties. On process control and SCADA security the 3rd Dutch event is outlined and a market analysis by Euro SCSIE headlines the results. An article on BCP and crisis scenario discusses the financing and the border of BCM in high impact low probability incidents.

Register for CRITIS now!

The CRITIS conference Series will continue with the 4th International Workshop on Critical Information Infrastructures Security in Bonn, Germany, Sept. 29-Oct 2, 2009 http://www.critis09.org. A resume of the last conference CRITIS'08, 13th to 15th of October 2008 in Rome is given. This should make the readers keen to attend this years' conference.

As always, selected links – mostly derived from the author's articles – and events conclude this issue.

When discussing 'business continuity', the editors of the ECN face a dark period as the funding and hosting of this newsletter is not guaranteed in the near future. Up till now, the ECN publication and web appearance were hosted by EU framework projects such as CI2RCO and IRRIIS. These projects have ended. The editors will continue at least with one addition issue and have tried to find alternative funding for the next years by approaching EU R&D directorates and ENISA. Until now, we have not been successful despite very positive reactions to the contents of and community building by the ECN. Ideas or help by our large reader community is appreciated. Despite those dark clouds, enjoy reading this issue of the ECN!

PS. *Authors willing to contribute to future ECN issues are very welcome. Please contact me or one of the national representatives. Further information about the ECN and its publication policies can be found in the introduction of the first ECN, see* www.irriis.eu.

CoMiFin: Middleware for Monitoring Financial Critical Infrastructure

The goal of the FP7 STREP project CoMiFin is to create a federated, distributed and collaborative network of agents for enhancing trustworthiness and dependability of financial infrastructures.

Barry P. Mulcahy

Dr. Barry P. Mulcahy is a Security Research Fellow for the Telecommunications Software & Systems Group (TSSG) at the Waterford Institute of technology (WIT). He received his BSc from University College Cork (UCC) in 2001 and his PhD in distributed security systems in 2008. He has worked as a lecturer in computer security at UCC and on a number of different national and international projects in the field of IT security. These include EI, SFI and FP7 projects. Barry is actively involved in the FP7 project CoMiFin: Communication Middleware for Monitoring Financial Critical Infrastructure. His research interests include secure workflows, distributed security, privacy and trust management systems. Barry regularly serves on technical programme committees and as a reviewer for conferences in his research areas.

e-mail: bmulcahy@tssg.org

Financial bodies, as well as businesses and ordinary people worldwide, are increasingly reliant on this financial infrastructure for conducting their day-to-day financial activities. As of today, the overall number of transactions being conducted over the financial ICT infrastructure amounts to millions per hour worldwide and several trillions of dollars/euros moved around the world every day. The SWIFT Circuit handled on 15th October 2008 (that years peak day): 17,860,068 messages, or approximately 206 messages per second on average.

An increasing amount of this traffic is being carried over publicly accessible communication media (such as the Internet), and involves commodity hardware and software. This trend towards the “webification” of critical financial services, such as home banking, online trading and remote payments provides for 24-hour service availability and improves user-friendliness. However, it exposes such services and the supporting ICT infrastructure to massive, coordinated Internet-based attacks and frauds that are not being effectively countered by any single organisation.

> **“One-in-a-thousand-year events seem to be happening annually, and one in a hundred year events are occurring weekly at the moment. All our risk models need to be reviewed, updated and re-applied”**
> **Lord Turner, February 2009**

The main purpose of the CoMiFin STREP is to strategically target the EU technological and institutional approach in financial infrastructure protection (FIP). Specifically, CoMiFin aims to provide “an infrastructure level monitoring, notification and mitigation” middleware as an essential element of FIP.

Threat Model

Several technologies and good practices enable thorough analysis of the events related to a specific domain, for example, the network traffic within an ISP. However, current monitoring approaches are inadequate to deal with coordinated and distributed attacks on a large scale. Even well protected and highly secure financial institution networks are vulnerable to complex and coordinated frauds involving multiple actors spread over different countries. In these cases, the monitoring and detection systems whose scope is limited to each individual organisation are unable to detect potential attacks and provide early alerts. To be effective, the monitoring activities have to involve multiple participants possibly distributed over disparate organisational, administrative and geographical domains.

The CoMiFin Approach

In CoMiFin, we have a long-term research agenda aimed at developing a comprehensive approach to financial infrastructure protection. In contrast to existing work, we do not restrict our attention to protecting each individual financial domain, but rather focus on the entire financial ecosystem as a whole. Our specific objective in the CoMiFin project is to devise a scalable distributed monitoring subsystem. This system will provide the relevant IT components of each participating financial domain with early notifications about faults and other potentially malicious activity originating at remote sites (possibly belonging to other critical infrastructures). Thus, enabling those components should trigger the necessary protective mechanisms in a timely fashion.

Financial actors collectively generate massive amounts of event data whose processing can no longer be effectively accomplished by existing centralised solutions. CoMiFin provides a distributed event aggregation and correlation system based on an unmanaged network infrastructure (the Internet), thereby providing resilience under failure scenarios including operational failures and deliberate breaches.

The primary objective of this *intelligence cloud* is to leverage the computational and storage resources available at each participant attached to the cloud in order to mine the event stream delivered for potentially dangerous patterns of activity and other anomalies. This is a non-trivial task requiring a holistic and cooperative approach across multiple elements of a financial infrastructure, such as disparate financial and telecommunication networks, various middleware platforms, and other interconnecting components.

The CoMiFin Technical Architecture

The vector for the next disruption or attack on financial CI is an unknown quantity. In order to be effective as an early warning system for financial CI, any system must be capable of identifying and disseminating information about emerging threats in real-time.

The CoMiFin architecture is a highly scalable and robust monitoring software system that enables consistent sharing of operational conditions amongst all of the inter-dependent parties including utilities providers, such as telecommunication service and electricity providers.

The system is designed to meet a variety of non-functional requirements, such as responsiveness, predictability, security and trust. Interfaces with existing network management systems deployed in individual financial domains (for example, various IBM Tivoli products) facilitate effective domain specific monitoring and management policies.

CoMiFin innovates across a spectrum of distributed computing technologies including (but not limited to): semantic overlay networking enhanced with trusted and secure group formation; highly scalable event processing; and new techniques for intrusion detection and mitigation strategies.

On joining the CoMiFin intelligence cloud, more secure agreements can be reached by subsets of participants. These interest-based agreements allow participants to subscribe to the so-called *semantic rooms*. These rooms are exclusive virtual spaces where participants can share interest-based events and information at a higher level of security. This could include information on fault notifications, service interruptions, DDoS and any other cyber-attacks.

The operational independence of financial actors is unaffected

The CoMiFin system is strictly an information sharing medium for all elements of financial CI. While actors in the system may be dependent on each other for services at a business level, the independence of their internal infrastructures and their freedom to act on information provided by CoMiFin is not affected by their participation in the system. This allows each actor to tailor their response to emerging threats based on local domain knowledge, the level of trust associated with the source of the information, and the relevance that they place in the information provided via CoMiFin. This real-time information support allows mitigation strategies to be implemented by financial actors in a timely and appropriate manner.

The CoMiFin Community

As part of the engagement process with the financial community, the project has close ties with the Co-ordination action project PARSIFAL, which purpose is bringing together the financial industry and research stakeholders in order to better establish trustworthy better protect CFI.

In addition, a Financial Advisory Board (FAB) has been established for the project. The CoMiFin FAB is chaired by Mr. Thomas Kohler of UBS Zurich and has members from across the European financial landscape. The board includes both national and international service providers and steers the project with their operative knowledge of CFI.

The CoMiFin Consortium is actively cooperating with the FAB and other financial bodies in the areas of: requirements analysis, regulatory policies, prototyping and assessment, and dissemination of the results.

The CoMiFin Consortium

The CoMiFin Consortium consists of 9 partners: ElsagDatamat (IT), Technische Universität Darmstadt (DE), IBM (IL), Waterford Institute of Technology (IE), Ministry of Economics and Finance of Italy (IT), OptXware (HU), KreditTilsynet (NO), University of Modena (IT) and Consorzio Interuniversitario Nazionale per l'Informatica (IT). This represents an ideal mix of commercial, academic and financial interests in the field of FIP.

If you would like to find out more about CoMiFin please visit our
website at www.comifin.eu or
email info@comifin.eu.

DIESIS – Designing a Research Facility for CIP

The EU funded project DIESIS investigates the feasibility of a new facility for joint research in Critical Infrastructures and their protection, supporting particularly modelling, federated CI simulation, and analysis.

Erich Rome

Erich Rome is a senior researcher at Fraunhofer IAIS, Sankt Augustin, Germany. He has a PhD in Engineering Sciences and is the co-ordinator of the EU project DIESIS.
emai: erich.rome@iais.fraunhofer.de

Sandro Bologna, ENEA

Sandro Bologna graduated in Physics at University of Rome. From 1972 up today he has been working at ENEA, as Researcher, Head of Research Units, as well as Head of Research Projects at national and international levels.

Erol Gelenbe

Erol Gelenbe is a renowned Professor at Imperial College, London, and author of several books and more than 120 top scientific publications. His research activities include Large Complex Critical Infrastructure Survivability.

Eric Luiijf

Eric Luiijf works as Principal Consultant at TNO Defence, Security and Safety, Netherlands. His research activities include CIP and distributed simulation.

Vincenzo Masucci, CRIAI

Vincenzo Masucci is a Senior Researcher and coordinator of research activities at CRIAI in Portici, Italy.

Research on Critical Infrastructures (CI) is a complex task facing many challenges. Particularly, the investigation of dependencies between different CI requires wide domain know-how, CI data, and almost always federated CI simulation. For this task, challenges include missing interoperability of CI simulators, availability of CI data and suitable analysis tools, and establishing an effective cooperation of researchers and stakeholders. The EU funded project DIESIS addresses these challenges by proposing to establish the basis for a European modelling and simulation research facility based upon open standards to foster and support joint European-wide research on all aspects of CI with a specific focus on their protection.

Introduction

CIs that are vital for a society and its economy, such as telecom systems, energy supply systems, transport systems and others, are getting more and more complex. Dependencies emerge in various ways, due to the use of information and communication technologies, legislation, market liberalisation, and other factors. The understanding of the complex system of CI with all their dependencies and interdependencies is still immature. Yet these systems need to be protected, for instance, against cascading failures that may affect several CI sectors. Research in the area of CI Protection (CIP) therefore has to rely on using simulation systems.

The goals of DIESIS are designing a new platform for joint research in CIP and fostering the development of new technologies for semantically interoperable federated CI simulation.

For simulating complex scenarios with dependencies between different sectors, typically heterogeneous federated simulations are used, but general modelling interoperability approaches or standards are missing.

The EU funded project DIESIS conducts a design study for a new research facility dedicated to joint research on Critical Infrastructures with a focus on their protection. The facility has the working title European Infrastructures Simulation and Analysis Centre (EISAC). According to the EU's ERA policy, it shall be organised as a pan-European research infrastructure. It shall offer technologies, data and services to researchers, operators of CI, makers of CI simulators, and governmental organisations and offices overseeing CI or ruling safety and security issues.

Design study

The goal of DIESIS is to perform a design study for EISAC enabling federated simulations of CI systems and supporting research on CIP. The establishment of such a distributed infrastructure in more than one country requires careful preparation. Thus, DIESIS is performing a thorough conceptual design study in order to prepare the establishment of EISAC. The work of DIESIS includes:

- Analysing in detail the requirements for EISAC coming from researchers, industrial stakeholders, decision makers and governmental organisations.

- Assessing the feasibility (scientific, technical, financial and legal) and the potential impact (scientific and technical) of EISAC.
- Developing a strategy and roadmap for the deployment of EISAC, including a business model, an organisational model of the operating entity of EISAC, a list of possible sponsors, a list of possible services to be offered, and a list of potential users and customers.

Technical work

The technical work of DIESIS comprises the following tasks: defining a set of requirements for the interoperability technology to be used for federated CI simulation, analysing available interoperability middleware, reviewing and characterising available CI simulators, developing a communication middleware and an ICT architecture for federated CI simulation, and, last but not least, identifying a process or workflow for setting up federations of CI simulators. A part of the technical concepts shall be demonstrated in a sample federation.

Communication Concepts

In order to support distributed federated simulation over various types of networks, a suitable communication middleware is required. One of the DIESIS project partners develops a quality of service enhanced communication middleware that shall work both via standard Internet (IPv4 and IPv6), high-speed networks like GÉANT [1], and private networks.

Essential communication requirements of distributed federations have been identified in order to guide the design of the communication protocols and algorithms. The most important communication requirements for large-scale federations have been identified as reliable and real-time (deadline-based) group communications. According to an evaluation of these requirements, a solution was proposed that groups all communications facilities required by the federates and the federation management system into a communication layer (CL). The CL is responsible for the delivery of federation messages under quality-of-service (QoS) criteria set by the communication requirements of the federation, also taking security and privacy aspects into account. An adaptive and reliable software architecture for the CL has been proposed that offers flexibility to support large-scale distributed federations and allows the incorporation of optimisation algorithms for group communications and security algorithms to provide communication security and privacy.

Ontologies of Critical Infrastructures

One part of the method to achieve semantic interoperability is the use of ontologies at different levels. On one hand, *Domain Ontologies* are derived from CI domain knowledge in order to formalise the conceptualisation of CI domains. They are tailor-made to the investigation at hand and depend, for instance, on the fidelity (or granularity) of the intended simulation. On the other hand, the concrete ontologies to be used are instances of *Domain Ontologies*. The instances are derived from available CI data, harnessed within the ontological conceptualisation of the domain. For each involved CI there must be at least one ontology. The simulators themselves and the federation may also require ontologies. Then, a *Federation Ontology* is realised to formalise the knowledge of cross-domain interconnections; while appropriate rules are defined to model the behaviour of those interconnections. A rule specifies the way two interconnected objects interact, allowing the propagation of effects from domain to domain. The rules are part of the implementation of the interoperability middleware. Additionally, when information needs to be exchanged between simulators in a federation that requires a transformation (e.g., transformations of units of measurements or coordinates, working ranges of parameters of infrastructure elements and so on), ontologies address the problem of the transformation factors. In general, rules and facts are stored in a knowledge-based system. Based upon a technology assessment, DIESIS has chosen to use a rule engine based on Jess for this task. A first publication describing this ontology concept has been presented at the IFIP WG 11.10 conference 2009 [2].

ICT Architecture

In the last decade, some powerful simulation tools emerged from several application areas related to CI. These tools are able to simulate technological systems (energy supply systems, telecommunication systems, railway traffic systems, …), logistic situations (military and civil operations, logistic chains, …) and common societal interrelations (e.g., economy simulations).

As a general rule, the involved simulators are closed system worlds. Typically, the design of these system worlds either disregarded the ability of coupling with other domain simulators or, in the best case, only to a very limited extent. Currently there are a number of projects that aim at coupling several stand-alone simulators in order to simulate large-scale systemic relations, like EPOCHS [3] and IRRIIS [4].

The market for simulator coupling middleware is dominated by highly proprietary solutions and differing implementations of a few standards like the High Level Architecture (HLA) for federated simulations. This situation leads to a strongly competitive acting of involved vendors. This adds to the problem of coupling simulators another – not primarily technological – dimension that makes the efforts of harmonising and coupling simulators even more difficult.

We concluded that purely generic approaches for coupling of simulators are not feasible from current state-of-the-art. The design space of “all possible simulators” in one application area, as for instance CI, is too large for making all required ICT-mechanisms available in a generic manner.

Thus, DIESIS takes a different approach towards coupling CI simulators. Architectural core concepts considered are:

- Scenario orientation. The first step for creating a federation of CI simulators for a given investigation or research task is the description of this task by means of a network of agents and application-oriented services. This network is then gradually transformed into a technological service network that guides the realisation of the federation.
- Lateral coupling of simulators, enabling the reuse of existing coupling solutions, e.g., if the simulators to be coupled are HLA compliant. If no solution for a certain coupling exists, a new one may be created and stored in a repository (taking into account possible sensitivities of the federation). This allows for a quick start for creating federations and will lead to an increasing inventory of coupling solutions.
- Distinguishing simulator couplings based on four different types of functions (data links, function links, time links, and control links). This leads to clearer design and facilitates the reuse of the coupling solutions.

Technical demonstrator

DIESIS will realise a demonstrator for a subset of its technical concepts, including communication concepts for distributed simulation, ontologies for CI, and the outlined ICT architecture approach for achieving interoperability of the federated simulators. The demonstrator will include an electricity network simulator (SINCAL, [5]), a telecommunication network simulator (NS2, [6]), a railway simulator (OpenTrack, [7]) and a simple flood simulator. The scenario to be simulated is the disruption of CI services in a large urban region in Europe due to local flooding.

Work on organisational, legal, and economic aspects

Core aspects of the assessment of the business feasibility are the assessment of possible organisational and legal forms of the pan-European research infrastructure EISAC, a description of possible products and services, the identification of target users and customers, and the assessment of the economic feasibility.

Organisational aspects

It is clear that EISAC should have several sites in different Member States, in order to be able to provide localised services, like know-how in the specifics of national CI, but also to be able to attract national stakeholders, agencies, and ministries for the intended collaboration in CIP. The sites should cooperate closely in order to use synergies. EISAC shall have a headquarter with strong relations to the national sites.

Legal aspects

It should be mentioned here that the creation of European research infrastructures (RI) is a strong policy of the European Commission. Currently, there are about 40 active projects designing or preparing the deployment of RI. All of them have to cope with their specific organisational, legal, and economic aspects. They need to clarify the statutory seat and the legal and organisational form – aspects that are not independent from each other. In order to facilitate the foundation of pan-European research infrastructures, the European Commission has adopted a council regulation on the Community legal framework for a European Research Infrastructure Consortium (ERIC, [8]). This legal form seems most suitable for EISAC and is compatible with the proposed organisational form. The legal form of an ERIC requires EISAC to be a not-for-profit organisation.

Economic aspects

The economic assessment part of the design study includes the identification of target users and customers, the identification and description of a business model for EISAC including a detailed description of products and services and customer benefit, and, last but not least, getting support from Member States. The currently discussed portfolio of EISAC offerings has been shaped both by the DIESIS consortium and potential users and stakeholders. The latter have been involved by sending out questionnaires and by holding a public workshop for receiving feedback on the initial portfolio.

The current portfolio discussed comprises – besides technology for semantic interoperability of distributed federated simulation – several repositories, additional tools, services, and consultancy.

Repositories may contain CI data (realistic or real), models, scenarios, reusable link implementations for coupling simulators, software prototypes of simulators and tools originating from CIP research, and more.

Additional tools may comprise analysis tools, tools for logging and visualisation, tools for model and scenario management, and more.

The tool and software suites offered by EISAC could also be made available to CI operators and security offices in order to be used for private simulations in a closed company or office network.

Consultancy could be provided for various topics, including domain know-how for several CI sectors, selection of suitable simulators, setup and management of federations and more.

Conclusion and Outlook

We have presented an overview of the work of the EU project DIESIS, which performs a design study for a new pan-European Research Infrastructure for CIP Modelling, Simulation and Analysis (MS&A). DIESIS is forming the basis for this facility, titled EISAC, by studying its technical, organisational, legal and economic feasibility.

The next steps within the duration of the DIESIS project will be the realisation of the technical demonstrator, a federated simulation of a scenario involving three CI simulators and a flood simulator. We will continue to invite potential users and stakeholders of EISAC to help shaping the services, tools and technology that EISAC shall offer. As far as the organisational, legal, and economic feasibility are concerned, DIESIS will agree on an organisational model that is compliant with a suited legal form, preferably an ERIC. An essential step towards realisation of EISAC will be the inclusion of EISAC in the research infrastructure roadmap of the European Strategy Forum on Research Infrastructures (ESFRI) [9], a body that provides support to policy makers of the European Commission. Inclusion of EISAC in the ESFRI roadmap and receiving national support by means of expressions of interest from governmental organisations in EU Member States are strategic objectives for the remaining project term. If DIESIS achieves these objectives, the realisation of EISAC might continue by entering a preparatory phase, followed by a construction phase and finally the deployment and operation of the facility.

Acknowledgments

The research leading to these results was funded by the European Community's Seventh Framework Programme FP7/2007-2013 under grant agreement n° 212830.

References

[1] GÉANT: Pan-European Gigabit Research and Education Network, http://www.geant.net/.

[2] V. Masucci, F. Adinolfi, P. Servillo, G. Dipoppa, A. Tofani: “Critical Infrastructures Ontology based Modelling and Simulation”, in: Proceedings of the Third Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, March 22–25, 2009.

[3] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, D.s Coury: EPOCHS: “A Platform for Agent-Based Electric Power and Communication Simulation Built From Commercial Off-the-Shelf Components”, IEEE Transactions on Power Systems, Vol. 21, No. 2, pp. 548–558, May 2006.

[4] R. Klein, E. Rome, C. Beyel, R. Linnemann, W. Reinhardt, A. Usov: “Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS”, in: Proceedings of the 3rd International Workshop on Critical Information Infrastructures Security, pp. 41–62, Frascati, Italy, October 2008.

[5] SIEMENS: SINCAL simulator, http://www.simtec-gmbh.at/sites_en/sincal.asp.

[6] NS2: The Network Simulator, http://www.isi.edu/nsnam/ns/.

[7] OpenTrack: Railway Traffic Simulator, http://www.opentrack.ch/.

[8] European Commission, *COUNCIL REGULATION on the Community legal framework for a European Research Infrastructure Consortium (ERIC)*, st 10603/09, Brussels, June 22, 2009

[9] ESFRI: European Strategy Forum on Research Infrastructures, http://cordis.europa.eu/esfri/.

DIESIS

DIESIS Project Information

Co-ordinator: Erich Rome, Fraunhofer IAIS, DE.

Project duration: 24 months

Email: diesis (at) iais.fraunhofer.de

More information can be found at the DIESIS website:

http://www.diesis-project.eu

DIESIS Consortium

Fraunhofer IAIS

CRIAI

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

Imperial College London

TNO

Developing a national CIP strategy: Swiss experiences and results

The Swiss government has approved a basic strategy this summer which provides the foundation for a full-fledged national strategy on CIP by 2012.

Stefan Brem

Stefan Brem received his PhD in Political Science at the University of Zurich in 2003. He leads the section on Risk Analysis and Research Coordination with the Swiss Federal Office for Civil Protection.
e-mail: stefan.brem[at]babs.admin.ch

Previously, he worked with the Federal Department of Foreign Affairs where he has co-founded and organised five workshops on Critical Infrastructure Protection (CIP) and Civil Emergency Planning (CEP) within the EAPC/PfP framework.

Information on the Swiss CIP Programme: www.infraprotection.ch

Switzerland - as many other modern societies - depends on a functioning network of infrastructure elements. "Critical" infrastructures are those that are especially important for the system as a whole or for other infrastructures. In Switzerland they are grouped into sectors, such as energy, transportation, or communication, and further subdivivded into sub-sectors (e.g. power, oil and gas supply in the energy sector). Disruptions of critical infrastructures may have severe consequences for the population and its vital resources.

In June 2009, the Swiss Federal Council approved a Basic Strategy for Critical Infrastructure Protection that will improve cooperation between the various authorities involved. The basic strategy lays out the general framework and applicable principles. Furthermore, it identifies four measures aimed at enhancing protection.

The Goal and Purpose of CIP

The goal of Swiss CIP activities is to reduce the likelihood of occurrence and/or the extent of damage incurred in a disruption, failure, or destruction of critical infrastructures at the national level, and to minimize the duration of downtime. Some sectors, and particularly some of the objects they contain (such as nuclear power plants or dams), already feature highly advanced protection measures. Thus, these aspects are not the main concern of CIP in Switzerland. Instead, the focus is on cross-sectoral coordination and a consistent approach at the national level.

The focus is on cross-sectoral coordination and a consistent approach at the national level.

First CIP Report in 2007

In June 2005, the Federal Council commissioned the Federal Office for Civil Protection (FOCP) to coordinate the CIP activities leading up to a national CIP strategy. Based on this mandate the FOCP set up a working group on CIP comprising all seven federal government departments and the Federal Chancellery. In 2007, the CIP working group produced a first report that was approved by the Federal Council. It sets out the key concepts and identifies ten critical sectors and 31 subsectors.

Second CIP Report in 2009

The second CIP report, of which the Federal Council approvingly took notice in June 2009, provides information on the activities conducted since the first report. These were mainly designed to enhance the understanding of this comparatively new subject matter. The report also indicates the further work that will be necessary in order to develop the national CIP strategy by 2012.

Concluded CIP Projects

In the framework of the CIP Programme several projects were conducted to improve the methodological setting, to develop a deeper understanding of the subject matter and to get insights for the elaboration of a national CIP strategy. The activities benefited from the knowledge and synergies provided by the CIP working group.

Case Study on Earthquake

The "earthquake case study" project provided an in-depth analysis of the effects of an earthquake on four subsectors in two different sectors (energy and transportation). This procedure made it possible to derive generally applicable insights for the basic strategy as it facilitated a study of cross-(sub-)sectoral effects and cascading effects. The investigation of several subsectors also allows conclusions to be drawn as to potential (inter-)dependencies.

Identification of critical infrastructures is of great social, political, and economic value.

The scenario was based on an earthquake of magnitude 6.9 such as the one that struck Basel in 1356. Subsequently, the study investigated the effects of such a severe earthquake in close collaboration with operators of critical infrastructure and cantonal experts. The analysis focused on the detailed assessment of the effects of such an earthquake on the infrastructure subsectors of power supply, oil supply, rail transport, and shipping.

These four subsectors had been selected on the basis of the previous assessment of failure malfunctions at the national level. The detailed damage assessment was followed by an evaluation of the results at the national level in terms of the remaining critical subsectors.

Expansion of Hazard Scenarios

In addition to the earthquake scenario, the first CIP report identified three other hazard scenarios (influenza pandemic, power outage, failure of the information infrastructure) that are of exemplary relevance to the CIP Programme. The aim of the study was to analyse the effects of the three scenarios on the critical (sub-) sectors. The three scenarios were based on previous work by other federal agencies and were each expanded in terms of the effects on critical infrastructures.

The analysis of the three scenarios showed that scenarios must be as standardised and up to date as possible in order to serve as the basis for future work in the framework of the CIP Programme.

Such scenarios will be elaborated by the "Risks Switzerland" programme that was approved by the Federal Council in December 2008. Furthermore, it became clear that the broadly diversified analysis of the effects of events on all critical infrastructure sectors should be combined with more in-depth analyses.

Identifying Critical Infrastructures

A methodology was developed to evaluate the criticality of the subsectors, with the magnitude of the impact of subsector failure being assessed in terms of three criteria, based on the assumption of an ordinary threat level.

The 31 critical subsectors were subsequently categorized into three criticality groups and listed alphabetically for each group. It should be noted that the criticality assessment explicitly avoided any statements on vulnerabilities, probabilities of failure, or the general significance of subsectors – for instance, during extraordinary events.

One of the insights of this assessment was that the identification and weighting of critical infrastructures is of great social, political, and economic value. A flawless, comprehensible, and broadly supported methodological approach is therefore essential.

Definitions

The main CIP terms have already been defined in the first CIP report and have been confirmed in the second report.

Infrastructures: The collective term "infrastructures" covers people, organizations, processes, products, services, and information flows, as well as technical and structural installations and constructions that, individually or as part of a network, enable the society, the economy, and the state to function.

These infrastructures are grouped into three levels:

- Sectors: e.g., energy, financial services, public health

- Subsectors: e.g., power supply, oil supply, natural gas supply

- Individual objects/elements: e.g., control centre for grid management, control systems, high-voltage power lines, dams, pipelines

Critical infrastructures: Critical infrastructures are infrastructures whose disruption, failure, or destruction would have a serious impact on public health, public and political affairs, the environment, security, and social and economic well-being.

Criticality: The criticality of an infrastructure refers to its relative importance in terms of the consequences that a disruption, failure, or destruction would have on the population and its vital resources.

Together with the (sub-)sector categorisation these definitions will be again thoroughly looked into at the beginning of the third phase of the CIP Programme.

Principles

The CIP Programme rests on five guiding principles.

Integral risk management: The integral risk management consists mainly of two parts: First, a detailed threat and risk assessment is performed, which then serves as the basis for measures in the following areas:

• Prevention (e.g., structural-technical or zoning measures)

• Preparation (e.g., contingency and business continuity planning)

- Intervention (e.g., alarm system, physical protection through security staff, standardized crisis communication)
- Recondition (e.g., temporary restoration of infrastructures)
- Reconstruction (e.g., of infrastructures)

All-hazards approach: The threat and risk analysis applies an all-hazards approach, i.e. all relevant hazards (natural hazards, technical hazards, social hazards and violence) are taken into account.

Resilience: Because it is impossible to protect all critical infrastructures permanently or to eliminate all vulnerabilities completely, resilience is of great importance. Generally, the aim is to return to a "normal" state as quickly as possible following an incident.

Maintaining proportionality: The selected measures should be reasonably proportional to the risk assessment and to the protection goals that are to be attained. Proportionality should also be maintained with regard to costs, protection, and security as well as liberty and legality.

Subsidiarity: Measures must be adopted both by the operators of critical infrastructures and by the public sector. Since approximately 80% of critical infrastructures are located in the private sector, the latter has a special responsibility for undertaking measures and investments of its own. The main responsibility of the public authorities is to protect their own critical infrastructures and to support operators.

Four Core Measures

The basic CIP strategy specifies the measures to be taken with regard to the protection of critical infrastructures:

Prioritizing Critical Infrastructures: In order to be able to use resources efficiently, critical infrastructures must be prioritized. In addition to the criticality assessment of the 31 subsectors, individual critical infrastructure elements will be identified and prioritized based on a standardized method and uniform assessment.

Resilience is of great importance as you cannot protect all CIs.

Protection through Comprehensive Approaches: Critical infrastructures are protected through comprehensive protection concepts that include specifications as to protection goals, protective measures, and implementation plans. The protection concepts relate to critical sectors as well as the infrastructure elements of national significance that are listed in the CIP Inventory. They complement the existing protection concepts in critical subsectors.

Improving Basic and Applied Knowledge: Basic and applied research in the field of CIP is of great importance. In particular, the high degree of interdisciplinarity involved must be borne in mind. In order to make optimal use of the CIP Programme's synergies, the studies cover cross-sectoral aspects such as scenario-based analysis of effects of various events in and across the various sectors.

Fostering Risk Communication: Frequently, awareness of the significance of critical infrastructures and the possible implications of failures is lacking. Therefore, the operators of critical infrastructures, corporate actors, and representatives of the federal administration as well as the general public are sensitized to possible risks and threats in connection with critical infrastructures and are informed about rules of conduct and ways of protecting themselves.

Expanding the Basic Strategy

In the basic strategy, the relevant actors are identified and the various forms of cooperation are presented. The basic strategy serves as a point of reference for the elaboration of the comprehensive national CIP strategy and lays out a common framework for the actors involved. It will be reviewed when the national strategy is formulated until 2012.

.

An Overview of Software Supply Chain Integrity

Providing assurance in ICT systems increasingly relies on ensuring consistent integrity practices across the whole supply chain, including software components.

Paul Kurtz

Executive Director of The Software Assurance Forum for Excellence in Code (SAFECode) http://www.safecode.org/

Email: write to:stacy@safecode.org

Introduction

Commercial software underpins the information technology infrastructure that businesses, governments and critical infrastructure owners and operators rely upon for even their most vital operations. For that reason, enterprise customers are rightfully concerned about the security of commercial software and the potential for its exploitation by those seeking to maliciously disrupt, influence or take advantage of their operations.

As the software industry has become increasingly globalised, questions have been raised about what additional product security and brand risk are introduced by the increased distribution of software development activities, how this risk should be assessed, and what proactive measures can minimise their occurrence.

Commercial software underpins the information technology infrastructure that businesses, governments and critical infrastructure owners and operators rely upon for even their most vital operations.

These questions are of interest to suppliers and customers alike and have recently been aggregated under the label of "software supply chain integrity."

However, the concept of software supply chain integrity and its key components of "software integrity" and "software supply chain" are not clearly defined, thus creating significant challenges for customers and suppliers working to identify, compare, communicate and evaluate software integrity good practices. Recognising this gap, SAFECode has developed the first industry-driven framework for analysing and describing the efforts of software suppliers to mitigate the risk of software being compromised during its sourcing, development or distribution. This article is excerpted from the framework and can be obtained at http://www.safecode.org.

What is Software Integrity?

Software integrity is an element of software assurance, which SAFECode defines as "confidence that software, hardware and services are free from intentional and unintentional vulnerabilities and that the software functions as intended."[1] Software assurance is most frequently discussed in the context of ensuring that code itself is more secure through the application of secure software development practices.

However, eliminating software vulnerabilities through secure development practices represents only one aspect of software assurance. Another key consideration is the security of the processes used to handle software components as it moves through the software supply chain.

[1] SAFECode, "Software Assurance: An Overview of Current Good practices," February 2008.

In practice, software assurance involves a shared responsibility among suppliers, service and/or solution providers, and customers encompassing three areas:

- **Security**: Security threats are anticipated and addressed in the software's design, development and testing. This requires a focus on both quality aspects (e.g., "free from buffer overflows") and functional requirements (e.g., "passport numbers must be encrypted in the database").
- **Authenticity**: The software is not counterfeit and customers are able to confirm that they have the real thing.
- **Integrity**: The processes for sourcing, creating and delivering software contain controls to enhance confidence that the software functions as the supplier intended.

Software integrity practices are essential to minimising the risk of software tampering in the global supply chain.

The Challenge to Software Integrity

Governments, businesses and consumers purchase ICT solutions (systems, products or services) that are a complex collection of inter-related components assembled from hardware, software, networks, cloud services and outsourced operations. Throughout an IT solution's lifecycle, which can extend over more than a decade, many individuals have legitimate access to its components and operations.

The intentional insertion of malicious code into software during its development or maintenance is often referred to as a supply chain attack. A supply chain attack can be directed at any category of software, including custom software, software delivering a cloud service, a software product, or software embedded in a hardware device.

Software is packaged as a collection of files. To be successful, a software supply chain attack must result in either: a) the modification of (an) existing file(s); or, b) the insertion of (an) additional file(s) into the collection of software files.

Software integrity includes the controls in the processes for sourcing, creating and delivering software that ensure confidence that the software functions as the supplier intended.

Reports[2] that have considered supply chain attacks have concluded that: 1) there is no one way to defend against all the potential attack vectors a motivated attacker may identify; 2) focusing on the place where software is developed is less useful for improving security than focusing on the process by which software is produced and tested; and 3) there are circumstances when the insertion of malicious code would be almost impossible to detect.

It is important to recognise that while there is a risk that someone with malicious intent could attack software during its development, experts[3] have concluded that supply chain attacks are not the most likely attack vector. For example, the practice of hackers or other malicious actors finding and exploiting existing vulnerabilities remains the most common method of attack.

Software Integrity Control Points

Sophisticated ICT solutions have much in common with other engineering undertakings. Each ICT solution is a collection of components. Each component or its parts can be: a) developed by its supplier or on that supplier's behalf by their subcontractors; or b) licensed to the supplier by another vendor or obtained from Open Source repositories; or c) acquired outright by the supplier.

Yet, this complexity can be organised. ICT suppliers have natural control points within software supply chains. To identify these, consider that each software supplier controls three links of the supply chain. For these three links each supplier takes similar actions:

1. **Supplier Sourcing**: Select their sub-suppliers, establish the specification for a sub-supplier's deliverables, and receive software/ hardware deliverables from sub-suppliers;
2. **Product Development and Testing**: Build, assemble, integrate and test components and finalise for delivery; and,
3. **Product Delivery**: Deliver and maintain their product components to their customer.

As such, suppliers have an opportunity to apply integrity controls at each of these key links in the supply chain. For instance, a supplier can conduct acceptance tests on components received from their suppliers, and release tests on the components they deliver to their customer.

To be effective in today's complex global supply chains, software integrity processes and controls must be designed to be independent of geography,

[2] "Mission Impact of Foreign Influence on DoD Software," U.S. Defense Science Board, September 2007. "Foreign Influence on Software: Risk and Recourse," Center for Strategic and International Studies, March 2007. "Framework for Lifecycle Risk Mitigation For National Security Systems in the Era of Globalization," U.S. Committee on National Security Systems, November 2006.

[3] "Mission Impact of Foreign Influence on DoD Software," U.S. Defense Science Board, September 2007. "Foreign Influence on Software: Risk and Recourse," Center for Strategic and International Studies, March 2007.

accommodate diverse sources of software components, and extend from a vendor's suppliers to its customers.

Suppliers are aware of threats to their products and are, consequently, extremely protective of their code base – not only is the integrity of their products at stake but also their highly valuable intellectual property and brand. As such, suppliers delivering software have significant experience implementing powerful management, policy and technical controls that reduce the risk that their code can be compromised.

Yet, while individual software companies have integrity assurance programs in place, there has been little industry-led effort to identify and share good practices for implementing integrity controls or to provide customers with more clarity into how the industry is addressing this issue.

This is a critical gap that SAFECode is currently addressing with a focused effort to identify the threats, assess the risk, share current practices for mitigating the risk, and develop process guidelines that other software companies should consider adopting to protect the integrity of the software they produce through the global supply chain.

The adoption of well-defined and industry-developed software supply chain integrity practices should ultimately lead to increased customer confidence in the security of ICT solutions.

3RD Dutch Event on Process Control Security

This event „Control IT“concentrated in joint efforts to control the security of process control system in critical infrastructures and to empower the security managers.

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl

On June 4th, 2009, the third Dutch Process Control Security Event took place in Amsterdam. The event, organised by the Dutch National Infrastructure against Cybercrime (NICC), attracted both Dutch process control experts and members of the European SCADA Security Information Exchange (Euro-SCSCIE). A set of plenary sessions and parallel workshops addressed a wide range of topics. Seán McGurk of the US Department of Homeland Security discussed in his keynote speech the US Process Control Security programme. Later, in a subsequent workshop, he answered a set of questions by the audience about cyber crime and the benefits of international cooperation. Nate Cube, Wurldtech, discussed the cyber vulnerabilities of process control systems based upon the Industrial Cyber Security Vulnerability Database. A set of parallel workshops followed. An adjacent article highlights the outcome of the SCADA security questionnaire by EuroSCSIE. Another workshop focussed on the human behaviour aspects in information security. Responsibility alone is not enough to address the cybercrime issues; ownership is the key! Both personnel and management need to be closely associated with addressing cybercrime. Another workshop discussed how one can convince management. The secret: let them feel a little less comfortable and a little bit more insecure.

Since early 2009, the NICC works on a Dutch national roadmap to secure process control systems. The US roadmaps are considered as examples. The Dutch approach will be a cross-sector approach with a very practical aim. The first contours were sketched. The roadmap centres on the end user and will be very pragmatic. The intent is to complete the roadmap in 2009 and have it agreed by a broad range of stakeholders: manufacturers, system integrators, service organisations, end users from the critical sectors, government agencies, and research and development. The objective of the roadmap will be that in eight year's time any unauthorised use of process control systems cannot lead to serious disruption of critical infrastructure supply. One aspect will be incident registration of cyber security incidents in process control/SCADA systems. It was indicated that such a registration will start in September 2009 on trial basis.

At the end of the event, Annemarie Zielstra and Seán McGurk signed an agreement which allows Dutch public and private parties to take part in the DHS Industrial Control Systems Cyber Security Advanced Training which includes a red team/blue team exercise. The training will take place in November, 2009.

All attendees were very pleased with the interaction they had with their colleagues from other companies and the content of the workshops. They are looking forward for the 4th Process Control Systems Security event.

Process Control/SCADA system vendor security awareness and security posture.

A starting point for the adequate security of process control/SCADA systems is the security awareness and security posture by the manufacturers, vendors, system integrators, and service organisations. The results of a short set of questions indicate that major security improvements are required in this area.

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands. Member of the NICC team.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl

Dr. Stefan Lüders

As deputy computer security officer, Stefan is responsible for the security of the process control systems at CERN, Switzerland.
Phone +41 22 767 4841
e-mail: Stefan.Lueders@cern.ch

The third Dutch Process Control Security Event was held in Amsterdam, on June 4th 2009. The event, organised by the Dutch National Infrastructure against Cybercrime (NICC), attracted both Dutch process control experts and members of the European SCADA Security Information Exchange (Euro-SCSCIE). A set of plenary sessions and parallel workshops addressed a wide range of topics. These included the control systems security program in the United States, the first industrial cyber security vulnerability database, vendor requirements, ownership in process control security, and the development of the Dutch national roadmap to secure process control systems.

„There is no market demand for process control/SCADA security“.

Another topic which we will describe here in detail was the EuroSCSIE questionnaire on the security awareness and security posture of process control/SCADA manufacturers, vendors, system integrators, and third party service organisations.

EuroSCSIE

Stefan Lüders presented the background on EuroSCSIE. To better understand and control threats and vulnerabilities in process control/SCADA systems and networks, several nations and organisations started the EuroSCSIE in 2005. Its objective is *„to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions in the SCADA and Control Systems environment...*" with *"… those European Governments, Industry and research institutions that are dependent upon and, or whose responsibility it is to improve the security of SCADA and Process Control Systems.*"

Currently, EuroSCSIE has 19 members from 13 European nations representing users from various sectors as well as key government agencies.

Scary security tests

Stefan continued by showing the results of a 2005-2007 CERN study on the inherent security of 31 process control/SCADA devices from seven different vendors. Using the standard Nessus vulnerability scanner 17% of the process control devices crashed and required a full restart.15% failed partially, i.e. some communication services (e.g. FTP, Telnet, HTTP) hang up. The system vendors were rather clueless on how to react as "*There is no market demand for security*".

The setup of a questionnaire

Based upon a discussion within the EuroSCSIE about these and equivalent types of results in other organisations, an initiative was started to ask manufacturers, vendors, system integrators, and service organisations about their process control/SCADA security awareness and security posture.

In a quick approach, a simple questionnaire with open questions was developed by the EuroSCSIE members comprising four topic areas:

- General Security Aspects (security policies, standards, good practices),
- Device Security (robustness, system hardening, testing, certification, documentation),
- Software and Firmware Security (software development life-cycle, authentication & authorisation, patching & compliance, configuration),
- Support (technical assistance, confidentiality, vulnerability disclosure, trustworthiness of personnel).

Some manufacturers and vendors ducked specific security questions.

Each of these areas contained three to ten topics. For each topic, a couple of open sub questions were asked. For instance: "Which general security standards is your company following?", "Which control system security standards is your company following?", or "Is your company involved in developing standards?"

The questionnaire, supported by 93 different utilities and bodies such as the EuroSCSIE, the Dutch ISACs, Swedish FIDI-SD, Swiss MELANI, and the U.K. SCSIE, was mailed by these bodies to a large set of Process Control/ SCADA manufacturers, vendors, and system integrators.

Analysis of the responses

Only nine process control/SCADA system manufacturers, vendors, and system integrators returned the questionnaire. The NICC took the responsibility to analyse the results in an anonymised way. The full, detailed information has been provided to the EuroSCSIE members on basis of non-disclosure.

When analysing the completed questionnaires, it immediately became obvious that using open questions does not help to obtain answers that one can compare easily. Some respondents replied with half a page text per topic. One had to make educated guesses in which way the text answered to the stated questions. In some cases, it was obvious that the respondent deliberately wanted to avoid answering a detailed question. In other cases, it turned out that the stated questions were ambiguous. It did not help either that some questions seemed to be replicated where a strict delineation between hardware, software, and services was intended. Above all, open questions allow for vague and foggy answers. For example, the answers to one particular question ranged from a discussion of the availability of a non-disclosure agreement to the description of burning a CDROM of the complete software installation. Moreover, some vendors offer different product lines with different security characteristics.

In hindsight, some important questions were not asked for and therefore not addressed, e.g. software escrow, non-disclosure with 3rd party personnel and protection of customer data, information to customer when malware is detected in the service/maintenance organisation, audit trail of remote 3rd party activities, and secure disposal of failing storage devices.

For the aforementioned reasons, a future follow up of the questionnaire will mostly contain closed questions with some open boxes for additional remarks or explanations. Nevertheless, some conclusions based upon the limited set of returned questionnaires could be drawn and are discussed in the following.

General security aspects

The security policies of the respondents show a large variety in the level of maturity: from a formal global security policy to the reply that security is the issue of the end-user, not that of the PCS/SCADA manufacturer.

The questionnaire asked for the used of standards. Apart from ISA SP99, the ISO/IEC 17799:2005/27000 series, and ISO/IEC15408), some respondents comply with a large set of other (de facto) standards such as CIP 002-009, IEC 62351, IEEE 1711, NIST SP 800-82, CIGRE, …. Larger manufacturers support more standards and often co-operate in the development of industry standards.

Five of the respondents engage the Cyber Security Procurement Language for Control Systems (CSPL) in a positive way and regard it as the basis for security requirements of the customers. However, one respondent replied that the CSPL is used by end users in the wrong way, but did not explain what is wrong. Three respondents never heard about the CSPL, another one did not answer this question at all.

Device security

Five respondents have a formal development process in place, including code review and formal quality management processes. Three respondents trust the good craftsmanship skills of their personnel, but lack a formal process. One respondent outsourced this issue to 3rd party network security.

Systems can be hardened at additional costs by some of the respondent organisations, and three respondents have their systems externally certified or independently tested. One respondent pointed to external parties which offer verification; device security is not of their concern.

In order to assess whether the systems are robust, six respondents use common test tools such as Nessus and NMAP. Three use other tools such as Metasploit, Achilles test box, and protocol fussers. Since the 2005-2007 experiences by CERN, which we discussed before, the industry has moved. None of the respondents wants to publically disclose their test results. However, in a confidential setting, most customers will be allowed to take a look at the test results.

Regarding the support for secure IP- protocols in the process control/ SCADA environment, four respondents use and support protocols such as SSH, SSL/TLS and IPSec. Four respondents do not support them and one uses a proprietary protocol.

> **“Information security is an issue of the end-user, not of the PCS/SCADA manufacturer”**

The support of the end users by providing security documentation varies a lot with respect to the document quality and information content. It ranges from installation notes to a complete system security manua1. One respondent even offers a security test plan. Three vendors do not provide much security documentation but advertised the service of their in-house security consultants.

Only five of the respondents have a formal process for providing security advisories. Some of the others consider this. One manufacturer/vendor does not plan for providing security advisories.

PCS/SCADA software security

Access control and authentication most often depends on Microsoft Active Directory, others support mechanisms based on Kerberos, Radius, and LDAP. On the other hand, one respondent stated that they support only simple passwords and another respondent proudly mentioned the use of a **single unchangeable password**.

Patching is another hot topic in the process control security environment. The responses were quite diverse. One respondent does not support patching but issues a new release every six months. Another respondent verifies and officially supports a MS released patch within three to four days on average, and seven days maximum. Six respondents have patch verification and patch support processes in place. Nevertheless, most respondents state that their process control software is independent of the operating system. One respondent requires hardening of the underlying operating system and network software.

Transferability of the process control software and its licenses to another platform in case of hardware failure is supported by all manufacturers/ vendors, either by supplying new license keys, by moving a dongle, or by support via telephone.

Support organisation

The support/ maintenance organisations of the respondents have a quite diverse policy when hiring personnel. It ranges from a formal vetting procedure to trust on ‘blue eyes’. Some respondents have a ‘secrecy’ paragraph in the contracts with their personnel.

However, strong guarantees on the confidentiality the customers’ data were lacking in many cases, especially when that sensitive data is located at the manufacturer/vendor premises.

The laptops and other systems in use by the support/maintenance personnel are provided with a decent antivirus tool with up-to-date signatures. However, seven respondents do not have a policy or guarantees that their software patch level is up to date. Only one support organisation has a strict policy for their support people: “*Thou shall not connect to an end-user network of a customer*”.

Conclusions

Despite the limited set of responses, a number of security issues to be worked on by process control/SCADA manufacturers, vendors, system integrators, and third party service organisations stand out from the analysis:

- Industry good practices are required to guarantee business continuity in case of device failure. Licensing issues shall not block/delay the business continuity.
- Customers shall not drop security demands from quotations to reduce acquisition cost.
- The delivery of hardened system shall become industry standard.
- Access rights shall default to DENY. Default installation passwords shall not exist.
- Industry good practices are required for publishing patches and advisories, and to communicate vulnerabilities.
- Strong guarantees (industry good practices) have to be developed for the trustworthiness of support and maintenance personnel (and the full 3^{rd} party chain) as well as their maintenance procedures.

The dialogue about security between end users and the process control/SCADA manufacturers, vendors, system integrators, and third party service organisations need to be intensified. The questionnaire has been a good start. A next, fully developed, more framed questionnaire may help to stimulate this dialogue and professionalism in securing process control/SCADA systems.

Critical Financial Institutions: Business Continuity Scenarios and Costs

This is the second article in a series of three on how a good practice in software engineering, Test Driven Development (TDD), could become also a good practice for BCP writing at CFIs. First article showed how compliance with the ECIP Directive requires strong BC management at CFIs. This article focuses on how to deal with high costs of some BC crisis scenarios. Last one will show how TDD could help.

Prof. César Pérez-Chirinos
Business Continuity Unit Manager
Banco de España
cepeche@gmail.com

Abstract

This article is the second in a series of three. The series summarises author's experience of successful application of Test Driven Development (TDD) principles in the implementation of the Business Continuity Management (BCM) System in a Critical Financial Infrastructure (CFI): a central bank. This approach has been also useful in other central banks, both in Europe and Latin America.

The full series includes: (i) a Context section, explaining why CFI should have a strong BCM Programme if they want to assure compliance with future revisions of the ECIP Directive[1], (ii) a BC Plan (BCP) Maintenance Issues section –this article-, showing common problems arising to keep the BCP updated, (iii) a TDD of BCPs section, showing how to use TDD-like approach to solve issues in section (ii); and a Conclusions section.

Costs of resilience are virtually unlimited. This article shows a possible approach to delimitate responsibilities for bearing these costs. CFIs top managers require such a clarification to avoid either overinvestment or becoming scapegoats.

The Limits of Security Oriented Business Continuity Management

After the September 11 attacks on the World Trade Center complex, focus of BCM changed from technology oriented Disaster Recovery Plans (DRPs) to a wider scope centred on safety of people running critical processes.

We can summarise this change of paradigm saying that top managers at that time could think something like: *We already know how to have IT continuity. Let's work on how to assure people's continuity for highly disruptive scenarios, protecting them (and us) against any threat.* This way of thinking had the benefit to bring to the toolbox of business continuity management some classical techniques of security officers, like threat intelligence, people oriented crisis management, and so on. But it had the collateral damage of some degree of self-deception: there are business continuity disruption scenarios (earthquakes, pandemics, etc) that can't be mitigated no matter how much you spend on classical security measures.

And then, Katrina destroyed New Orleans.

And business continuity main word changed from "full protection" to "resilience". This was a wise move of

[1] "Critical Financial Institutions, OSPs and Business Continuity Plans". ECN Vol. 5, No. 1, pp. 21-23; April / May 2009

humbleness: There will always be business continuity scenarios that you can't mitigate. The only practical way to deal with these scenarios is to think: *"If my organisation were fully destroyed, why and how it should be rebuilt? And who will pay for it?"*

It is fully out of the scope of these articles to discuss financial crisis, but as we are dealing with business continuity and CFI, you should note the parallelism between the sentence above and the arguments for bank rescue in current financial crisis approach. This is not casual: some financial crisis scenarios could trigger business continuity events (strikes, etc), and some business continuity events (failure of a CFI in running its operations for several days) could trigger financial crisis, potentially devastating in both cases. The good news is that crisis management skills seems so be shareable by both domains[1].

Should we Decide Investing to Protect Our CFI Against this Scenario?

To any conscious top manager, this is "the big question" in trying to balance costs of business continuity preparedness and the potentially destructive consequences of not being prepared if the evaluated scenario arises. This is the biggest maintenance issue of Business Continuity Plans, as changing threats and technology requires a continuous maintenance effort.

But unfortunately, as a clever ex-broker points out[2], nobody has been ever prized by avoiding problems that never happened, even if problems didn't arise just because somebody took some successful preventive measures.

Business Continuity Management at CFIs must go beyond impact scenarios that most organisations use. Real causes of impacting scenario could make useless alternate resources theoretically committed to your BCP

Finally, the personal "risk appetite" of top managers causes them either to invest or not in business continuity preparedness. Most of the times, the subjective scenario likelihood estimation is the root cause of such decisions.

A clear example of the above has been the preparedness of CFI for pandemic flu, before current A(H1N1) pandemic flu started this year.

Since the huge economical impact of SARS pandemic in Asia and Canada was evaluated, many global financial institutions, like the International Monetary Fund, have done a lot of warning advice, jointly with the World Health Organisation, on pandemic flu preparedness.

But, for many CFI top manager, this scenario was probably rated, at unconscious level, as "a Hollywood thriller" and logically discarded. What is worse, at time of writing, virus mortality is so low that more sensitive managers could be scorn by their more sceptical board partners about the return on the investment enabling massive tele-working or antiviral stocking. We face so the risk that next pandemic wave will take us in a lower level of preparedness.

The Limit of Impact Scenarios

We shouldn't be too severe with such managers. Daily managing a CFI is a very stressing and demanding job, and sometimes their advisors try to simplify complex issues in a one-page report that includes problem description and the solution suggested, so only a "go/no go" decision is expected from the manager.

There is no doubt that tactical management can hardly avoid such a summary approach. But we believe that proper BCM can't use this approach without significant risk of misunderstanding. And this is the case with impact scenarios of BCM.

Consider the typical high absenteeism rate impact scenario. Sure, your critical processes are interrupted because people are not there. Some BCM consultants will tell top managers that massive tele-working support is the appropriate mitigation measure, as it covers you against pandemic, heavy snow and the like.

But what happens if absenteeism were caused by employees, terrified by a medium intensity earthquake, leaving out in mass to collect children at schools or take care of their relatives, while the computers were running waiting for

[1] Since mid seventies, the Bank for International Settlements (BIS), has been closely watching this interaction:

The Basel Committee on Banking Supervision, hosted at BIS, included in its Basel II Framework (see http://www.bis.org/publ/bcbs128.htm) specific provisions on Business Continuity Management (BCM) and Operational Risk Management (ORM) issues in banks.

More specific BCM job has been done by the Joint Forum, also hosted by BIS (http://www.bis.org/bcbs/jointforum.htm), that published in 2006 its High Level Principles for Business Continuity (http://www.bis.org/publ/joint17.htm), expected to be adopted by all CFIs and its supervisors.

Last but not least, the BIS 78th Annual Report (2008) includes this revelling paragraph: *"And war games need to be played by those who would actually manage problems in real time. […]. Businesses and banks are expected to undertake business continuity planning in advance of trouble. Surely we should expect as much from policymakers."*

[2] Nassim Nicholas Taleb: *The Black Swan: The Impact of the Highly Improbable.* Random House, 2007.

users? This really happened at least once at a CFI in Europe.

So, if top managers don't have enough time to drill down to possible root causes of an impact scenario with you, be sure that they are fully aware about the residual risk that they are accepting when they decide about a BC related investment or strategy.

Who Should Then Decide The Responsibility Limits In This Scenario?

We tried to clarify this issue during the re-evaluation of residual risk accepted by a CFI covered by impact scenario based BCP. We used the US 2005 FEMA's *National Planning Scenarios*[1] document as a yardstick to check which detailed scenarios were covered by accepted impact scenario.

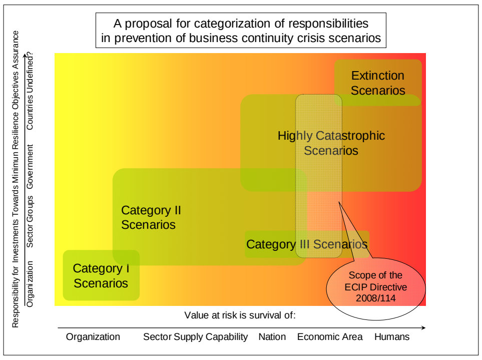
It was clear almost from the beginning of the re-evaluation exercise that most of such scenarios exceed what you can expect to be covered by a typical impact oriented strategy (main or alternate site fully unavailable, but not both impacted at same time).

At that point, some disturbing questions arise: if even such an expensive strategy doesn't cover your CFI, should you invest in a third site, or fourth one? As top manager, would you be liable in case of failure under such scenarios just because protection cost would be unaffordable from your, or the board, point of view?

And then, suddenly, we reach the most disturbing one: what would be the real demand of your services in such circumstances? Paradoxically, this question provides a guide to answer some of the hardest issues raised by extreme scenarios to CFIs: *only if your customers would continue demanding your services in an extreme scenario, you could be liable to invest in specific continuity investments to deal with it.*

We then started to classify the extreme scenarios in two categories. Category I scenarios refers to scenarios that don't impact too much outside your organisation limits. A big fire can fully destroy your main site, but it is expected that any wise manager should deal with this scenario in its BCM process, as external world is more or less harmless.

We then included in Category II the remaining scenarios, which clearly exceed CFIs capability to invest in its prevention: a nuclear bomb detonation, for example. It was clear that dealing with such high impact events must be done, at least, in cooperation with the full *critical* value chain: *critical customers-your critical processes-critical suppliers***.**


A proposal for categorization of responsibilities
in prevention of business continuity crisis scenarios
Responsibility for Investments Towards Minimun Resilience Objectives Assurance
Organization
Sector Groups
Government
Countries Undefined?
Extinction Scenarios
Highly Catastrophic Scenarios
Category II Scenarios
Category III Scenarios
Category I Scenarios
Scope of the ECIP Directive 2008/114
Value at risk is survival of:
Organization
Sector Supply Capability
Nation
Economic Area
Humans

As the above diagram shows, it was quite obvious that preventing the interruption of such a critical value chain requires, at least, some degree of sector agreement. Otherwise, BCM aware suppliers won't be competitive due to bigger investments in resilience.

In case of CFIs, the critical value chain includes a full variety of public and private stakeholders, so some degree of public regulation (at least, strong recommendations) should be established to assure that resilience objectives for financial sector are meet at medium and long term. Due to its global scope, it is also clear that international cooperation is a must, and the ECIP Directive seems to have a clear role in the solution of the problem of assignation of resilience costs.

Thinking the Unthinkable

However, we also realised that some scenarios could have special impact on some CFI, like legal or *de facto* single suppliers –some clearing houses, or even central banks having their own currency- that could face what we call Category III Scenarios. This scenarios would arise if such CFI were impacted by a Category II scenario but, due to its single supplier status, it were requested to provide its services –i.e., cash distribution- at emergency levels that could be ever more demanding than habitual ones.

It seems to be clear that resilience investments for Category III scenarios require explicit political actions to mandate such CFIs to be prepared to react. Otherwise, such investments would be easily blamed of wasting taxpayer's money. Finally, we also realise that other scenarios (labelled as "Highly Catastrophic" and "Extinction" ones) seems to be clearly out of current scope of BCM, as there seems not to exist a proper political instance able to assume formally this residual risk or the huge costs of its prevention. But to be honest, BCM practitioners, we should explicitly communicate the limits of our discipline.

Next Issue

In next, and last, article of this series, we will assume that you have a BCM budget in line with the CFI's risk appetite, and will discuss how to use Test Driven Development to avoid waste it with "paper" business continuity plans.

IPR and Disclaimer

This article is a research item of the on going PhD Thesis at Oviedo University of its author and does not express a position of Banco de España on the subject.

[2] An updated version can be found here: http://www.fema.gov/pdf/government/npg.pdf (pg. 31)

CRITIS'09 – Call for Participation

The 4th International Workshop on Critical Information Infrastructures Security takes place in Bonn, Germany, from September 30th to October 2nd, 2009.

Venue:

Bonn, Germany

Bonn is the former capital of the Federal Republic of Germany, hosting six ministeries and several security-related federal offices and agencies.

Günnewig Hotel Bristol

The workshop hotel is located in Bonn's city centre, just a three minutes walk from the main railway station and bus terminal.

Background and Scope

Critical Infrastructures are today of central importance for all developed countries. At the same time, Critical Infrastructures undergo rapid changes in many respects. Globalisation and liberalisation with their economical, social, technological and political aspects result in more and more interoperable, integrated and dependent Critical Infrastructures. These phenomena and the actual socio-political instability pose new and very hard challenges to the management and protection of these systems and, more specifically, imposes the development of innovative strategies to guarantee their service continuity. The abundance of services of modern infrastructures is no more thinkable without information and communication technologies (ICT). Though being key enablers of Critical Infrastructures, ICT are - at the same time - reckoned among the most vulnerable elements of the whole system constituting themselves Critical Information Infrastructures.

Information and communication technologies are not just key elements for Critical Infrastructures - with their general purpose approaches they also provide the ground for analysis, modelling, and simulation of Critical Infrastructures. Sophisticated information modelling and information integration techniques, new service, agent, or constraint based software engineering approaches, the next generation internet with its standard languages and tools will considerably influence the way Critical Infrastructure research will be done in the future.

Networking and Research

CRITIS'09 brings together experts from science, industry and public authorities involved in management, supervision and protection of Critical (Information) Infrastructures to provide an interdisciplinary and multi-faceted view about future security strategies for Critical (Information) Infrastructures.

The workshop is interesting not only as a forum for getting aware of recent research work in the area but also as an opportunity for sharing knowledge and for creating research networks to develop international collaborative projects.

Invited Speakers

James P. Smith, Los Alamos National Laboratory, NISAC Project Leader (USA)
"Large-scale Modeling & Simulation of Critical Infrastructure"

Dr. Milos Svoboda and Alla Heidenreich, SIEMENS AG, (Germany)
"Secure ICT Infrastructure for the future power grid at the example of E-DeMa project"

Dr. Michael Pilgermann, German Ministry of the Interior (Germany): "German strategy regarding CIIP"

Paul Nicholas, Director of Global Security Strategy, Trustworthy Computing, Microsoft Corporation
"Managing Risk in Critical Information Infrastructures"

Dr. Orestis Terzidis, SAP AG, Vice President, CEC Karlsruhe (Germany)
"The Internet for Energy – Perspectives and Challenges"

Programme

Presentation sessions: Invited talks plus oral presentations of reviewed papers

Poster and demonstration session: Reviewed posters and invited demos and posters

Panels:
"Simulation Platforms for Dependency Analysis of Critical Infrastructures" (Chair: Robin Bloomfield)
"How to link C(I)IP R&D EFFECTIVELY with the EU EPCIProgramme and national CIP R&D and policies?" (Chair: Erol Gelenbe)

Social events: Reception at Hotel Königshof (September 30), workshop dinner (October 1), sightseeing tour to Cologne (October 3, sufficient number of requests provided)

The detailed advance programme is available on the CRITIS'09 web site at http://www.critis09.org/

Venue

The city of Bonn is located in the heart of Europe with excellent reachability. The former German capital still hosts six of the German federal ministries, plus many security related offices, including the German Federal Network Agency and the German Federal Office for Information Security (BSI). Bonn is also the headquarters of German Telekom, T-Mobile, and the German Post.

The venue of CRITIS will be the Günnewig Bristol Hotel, located in Bonn's city centre, just a three minutes walk from the main railway station and bus terminal.

Chairs

General Co-Chairs: Stefan Wrobel, Fraunhofer IAIS and University of Bonn, Germany, and Costas Lambrinoudakis of the University of the Aegean, Greece.

Local Chairs: Uwe Beyer (Local Chair) and Rüdiger Klein (Local Co-Chair), Fraunhofer IAIS, Germany.

PC Co-Chairs: Erich Rome (Fraunhofer IAIS, Germany) and Robin Bloomfield (City University London and Adelard, UK)

Information

CRITIS'09, the 4th International Workshop on Critical Information Infrastructures Security, will take place in Bonn, Germany, from September 30th to October 2nd, 2009.

More information is available at the CRITIS 2009 web site: http://www.critis09.org

Registration

Registration information is available at http://www.critis09.org/

Online registration and registration by fax +49-2241-14-2381 are supported.

ECN-13 Selected Links and Events

Upcoming CIIP Conferences in Europe

- *2nd summer school on Network and Information Security (NIS'09) 14-18 September 2009 Crete, Greece is organised by the European Network and Information Security Agency (ENISA) and the Institute of Computer Science (ICS) of the Foundation for Research and Technology - Hellas (FORTH) The theme of the summer school is "Privacy and Trust in a Networked World: http://cordis.europa.eu/fp7/ict/security/events_en.html*
- *5th International Conference on IT Security Incident Management & IT Forensics, September 15th to 17th, 2009 Stuttgart, Germany http://www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf/imf2009*
- *4th International Workshop on Critical Information Infrastructures Security Bonn, Sept. 29-Oct 2,2009 http://www.critis09.org*

European Funded Projects

- CoMiFin: Middleware for Monitoring Financial Critical Infrastructure: www.comifin.eu
- DIESIS – Designing a Research Facility for CIP: The EU funded project DIESIS investigates the feasibility of a new facility for joint research in Critical Infrastructures and their protection, supporting particularly modelling, federated CI simulation, and analysis. www.diesis-project.eu
- FP7 PARSIFAL Coordination Action project brings together CFI and Trust and Security research stakeholders contributing to the understanding of CFI research and development challenges: http://www.parsifal-project.eu

Selected Links from Articles of this issue

- Information on the Swiss CIP Programme: www.infraprotection.ch
- GÉANT: Pan-European Gigabit Research and Education Network, www.geant.net/
- NS2: The Network Simulator, /www.isi.edu/nsnam/ns .
- OpenTrack: Railway Traffic Simulator, www.opentrack.ch/
- The Software Assurance Forum for Excellence in Code (SAFECode) www.safecode.org/
- Assessing and Improving SCADA Security in the Dutch Drinking Water Sector: www.springerlink.com/content/8l75v33245418j76
- European SCADA and Control System Information Exchange EuroSCSIE: *https*://espace.cern.ch/EuroSCSIE/default.aspx
- More specific BCM job has been done by the Joint Forum, also hosted by BIS www.bis.org/bcbs/jointforum.htm, that published in 2006 its High Level Principles for Business Continuity www.bis.org/publ/joint17.htm, expected to be adopted by all CFIs and its supervisors.
- FEMA's National Planning Scenario: www.fema.gov/pdf/government/npg.pdf
- *Technical details on actual research projects: http://cordis.europa.eu/fp7/ict/critinfpro/projects_en.html.*
- *Microsoft security advice: http://www.microsoft.com/security/default.mspx*
- *The Trustworthy Computing Security Development Lifecycle: http://msdn.microsoft.com/en-us/library/ms995349.aspx*
- *End-to-End Trust vision SAFECode: http://www.microsoft.com/mscorp/twc/endtoendtrust/default.aspx*