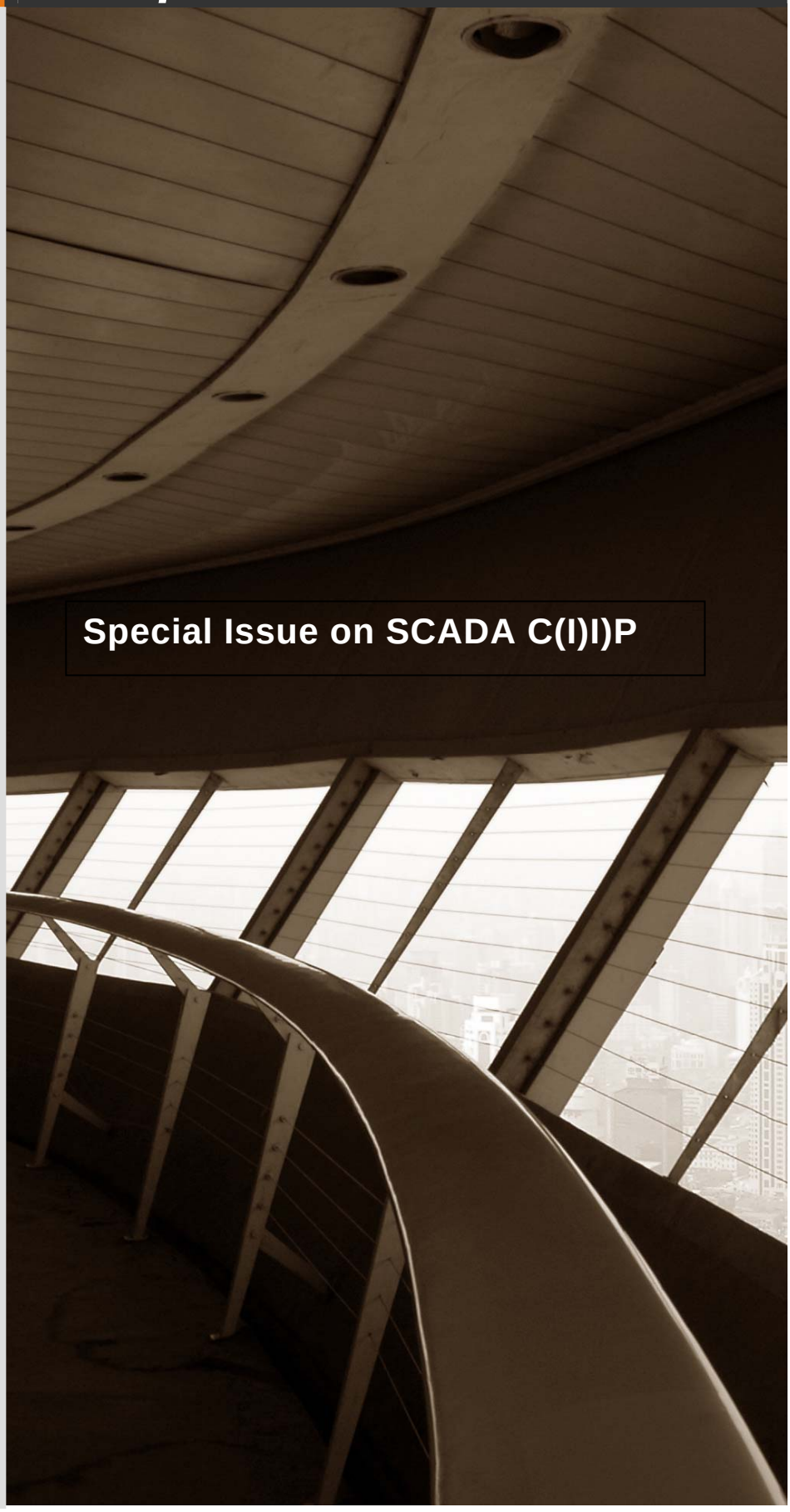
March / April 2008, Volume 4, Number 1

ECN

European CIIP Newsletter



Special Issue on SCADA C(I)I)P

IRRIIS

> 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, 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

>Founder and Editors
Eyal Adar CEO iTcon, ***eyal@itcon-ltd.com***
Bernhard M. Hämmerli, HTA, Initiator and Main Editor ***bmhaemmerli@acris.ch***
Eric Luiijf, TNO, ***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

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events

Applied research will be key for implementing C(I)IP

C(I)IP is now discussed for years at policy and conceptual levels. Meanwhile the problem of C(I)IP is well understood as the will to care for the infrastructure. However, practical solutions must be developed at the collaboration and technical levels.

Dr. Bernhard M. Hämmerli
Professor in Information Security
Founder of the Executive Master Program IT Security, FHZ
Vice-President ISSS Information Security Society Switzerland and Chair of Scientific and International Affairs

e-mail: bmhaemmerli@acris.ch
e-mail: bmhaemmerli@hslu.ch

Focussing C(I)IP

Making some thoughts about C(I)IP and observing its evolvement, new very practical projects on collaboration and technical issues are worked at, and discussed; e.g.:

- Development of test beds;
- Generating of test data;
- Initiating of ad hoc and working groups on technological issues such E-SCSIE
- Intrusion detection and / or organising collaboration.

The change form discussion level to implementation issues and research indicates a relevant evolvement of the topic; the necessary presumptions are met by now, to support society sooner or later with more resilient and robust infrastructures.

About this Issue

The EU centric conference CRITIS'08 is a major event for the C(I)IP community this year, because it is supported by IFIP, IEEE, IRRIIS and EU (DG JRC). We hope for many contributions and wish the organisers success.

A maritime security conference report from Bahrain's conference gives an overview on the topic and describes generally the relationship to C(I)IP.

The interesting recent USA publication of a monograph on critical infrastructure protection and risk is presented by the university researcher responsible for its development. Beside of common definition and understanding of terms seven additional study parts will be presented.

Three articles about SCADA Security are the focus of this issue: A general introduction to cyber attached control systems is followed by two contribution of British Petrol BP illustrating the practical meaning securing industrial SCADA systems for gaining resilience and robustness of critical infrastructures:

- The need of cross-sector and multi-national collaboration is discussed in the first article.
- Technical backgrounds and good practice examples are discussed in the second article.

The need and impact of digital identity systems in the context of C(I)IP is an essential issue to push information society forward in a secure way. Practical issues are discussed and a European electronic identity is proposed.

After five successful EAPC/NATO/PfP workshops on C(I)IP, the next workshop will be held first time collocated with the International Disaster and Risk Conference (IDRC) with the new name: 1st International Conference on Critical Infrastructure Protection and Resilience (ICCR 2008).

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.

Enjoy reading this issue of the ECN!

CRITIS'08 - 3rd International Workshop on Critical Information Infrastructures Security

The 3rd international Workshop on CI and their ICT from 13th to 15th of October 2008 in Rome, Italy wants to continue the success of its predecessors and seeks to attract researchers and professionals from all kinds of large critical infrastructures

CRITIS`08 Program Chairs

Stefan Geretshuber

IABG mbH, Germany
InfoCom, Safety & Security,
Dept. for Critical Infrastructures
geretshuber@iabg.de

Roberto Setola

University Campus BioMedico, Italy
Complex System & Security Lab,
r.setola@unicampus.it

Modern society's dependency on infrastructure services has been widely recognised. The abundance of these services is no more thinkable without ICT that therefore became a key resource. At the same time ICT is considered as being one of the most vulnerable elements of the whole system.

To continue with the success of its previous editions in 2006 and 2007, CRITIS´08 will bring together experts from science, industry and public authorities for the third time to provide an interdisciplinary and multi-faced dialogue about the third millennium security strategies for Critical Information Infrastructures and their protection.

Conference Scope

CRITIS´08 will host attractive presentations, poster sessions, invited talks and present high-quality peer reviewed papers focused this year on the following non-exclusive subjects:

- Modelling and Simulation of Critical Infrastructures;
- Interdependency Modelling and Analysis;
- Threats and Attack Modelling;
- SCADA / DCS and Control System Security;
- Self-healing, Self-protection, Self-management Architectures;
- Situation Awareness and Response Optimisation;
- CIIP Policy and Cross-Border Issue
- R&D Agenda, Benchmarking and Survey.

CRITIS´08 is co-organised by ENEA and by the Italian Association of Critical Infrastructures Experts (AIIC) and it is supported by the International Federation's of Information Processing (IFIP) Workgroup 11.10 on Critical Infrastructure Protection, the IEEE Computer Society Task Force on Information Assurance and the Joint Research Centre Ispra of the European Commission.

The workshop takes place at the marvellous location of "Villa Mondragone" in Frascati, Italy. Beautiful situated near Rome, Villa Mondragone has been the residence of Popes and famous families of the ancient nobility over the course of its long history. Today it offers with its wonderful gardens and magnificent view towards Rome an excellent and exclusive surrounding for CRITIS'08.

The CRITIS'08 organisation committee looks forward to receive various research and industrial contributions and of course would be glad to welcome you to the CRITIS´08 Workshop.

Paper Submission

Submitted articles that illustrate research results, R&D projects, surveying works and industrial experiences related to the subjects of the work-shop will be thoroughly evaluated by reviewers. As in the last years, it is planned that post-proceedings will be published by Springer in the *Lecture Notes in Computer Science* series. Extended and revised versions of the best papers, after a further peer-reviewed process, will be published, on the base of their arguments, in a special issues of the *International Journal of System of Systems Engineering* (by Inderscience) or in a special issue of the *International Journal of Critical Infrastructure Protection* (by Elsevier).

The ***deadline for paper submission is May 15th***. For submission instructions and more information see http://critis08.dia.uniroma3.it/.

Maritime Infrastructure Protection

The Maritime Infrastructure Protection Seminar held in Manama, Bahrain on February 26-28, 2008 raised a number of critical international collaboration and co-ordination issues

Stephen D. Wolthusen

Full professor of information security at Gjøvik University College, Norway, and Lecturer in the Information Security Group, Department of Mathematics at Royal Holloway, University of London

e-mail:
stephen.wolthusen@rhul.ac.uk

The maritime infrastructure by definition transcends national borders and is characterised by a large number of interacting parties ranging from governments, port authorities, and the players in the shipping industry to international regulatory bodies. As can be expected, the interests of the parties involved are not always perfectly aligned, requiring a careful balancing.

Threat Assessment

Following brief welcoming remarks by Vice Admiral Kevin Cosgriff, Commander, United States Naval Forces Central Command, a review of recent attacks on maritime infrastructure was presented by Dr. Michael Mullen. The maritime environment offers a rich selection of targets for deliberate attacks including off-shore installations such as oil and gas drilling and production rigs, and the transhipment terminals required for transporting oil and gas. Compared to such fixed installations, the risk assessment for infrastructure elements afloat is a more fluid process. The potential for damage to life and property as well as to the environment, however, can also be considerable as in the case of oil and chemical tankers, LPG and LNG carriers, or even nuclear fuel carriers.

Maritime Critical Infrastructure is by its very definition a multi-lateral and multinational endeavour

Documented attacks by sub-state actors have taken places anywhere from riverine environments to ports and territorial waters and all the way to the High Seas.

The resources at the disposal of attackers vary according to the size and sophistication of the respective organisations which range from localised criminal gangs and organised crime bodies to insurgents, terrorists, and in some cases even military or renegade military units. Under some circumstances, even the actions carried out by environmental activists can have severe adverse consequences.

Piracy is a long-running concern with vessels and cargoes being commandeered and in some cases entire ships being converted into so-called “ghost ships”, carrying illegal cargo. This, however, becomes a critical infrastructure concern when considering that such acts of piracy occur in areas that are difficult to navigate in such as in straits and shallow coastal areas with strong currents. Bad ship handling or deliberate sabotage can therefore lead to severely restricting the navigability of such areas, inducing disproportionate costs even when salvage vessels are available and can be dispatched quickly.

While terrorism has not claimed significant direct casualties or indeed costs, certainly not compared to acts of piracy, the financial costs involved can still be substantial. Attack on the 300’000 dwt tanker MV Limburg in 2002 not only caused massive damage to the vessel and the discharge of more than 90’000 tons of crude oil into the Gulf of Aden, but also had severe repercussions for trade with Yemen in general as insurance rates for oil products tripled and policy underwriters cancelled war insurance clauses. Among other things, this resulted in a

75% drop in port activity at the Port of Aden.

Given that the vast majority of goods are transported by sea and that this transport is also increasingly time-sensitive for many types of goods, even small disruptions can have severe repercussions. At the same time, the movements of merchant ships are highly predictable, and apart from calling on law enforcement and naval support, such vessels and installations have very limited defensive options.

At the same time there exists a conflict of interest between shipping safety and security. As outlined by CAPT McCarthy, USN, the Automated Information System (AIS) provides for an open information sharing platform on which vessel location, course, and other pertinent information is available worldwide. This system regulated and mandated by the International Maritime Organization (IMO), a body of the United Nations for passenger vessels and larger cargo vessels but in some countries applicable to other vessels as well, does not employ any cryptographic security mechanisms. Therefore, not only is the information on shipping movements readily available to anyone, but transponder identification codes and transmissions can be spoofed and injected trivially. This of course is a major concern in case hazardous or otherwise cargo is being transported and could also provide attackers with crucial information as to when and how to best attack ships en route.

Similar trade-off considerations were also mentioned by Mr. Moon from the U.S. Department of Homeland Security; sophisticated risk management must balance between freedom of movement and freedom of trade, respectively, and the need to conduct inspections and collect intelligence information which can spot adverse developments. One key element in the DHS strategy is to ensure that supply chains are not disrupted; to this end, close collaborations with industry such as in the U.S. Secure Freight Initiative are required. Here, as in many other areas involving maritime infrastructure, it is only through largely voluntary efforts that the desired goals can be achieved since key infrastructure components are under the control of private enterprise or located overseas.

The theme of public-private interaction and engagement was also echoed by Mr. Dale Davis; here, the discussion focused on the control that governments and the public at large can have over contractors of all types to prevent fraud, waste, abuse, and in some cases incidents that go beyond these.

Issues surrounding the protection of maritime infrastructure, particularly against subversion-type attacks were discussed by Dr. Stephen Wolthusen, (Gjøvik University College, Norway, and Royal Holloway, University of London, UK) who described the challenges to detecting sophisticated attacks against sensors and actuators in an environment that is more and more characterized by highly automated control systems with limited potential for manual supervision and intervention. This implies that operators have to rely more and more on what control systems are reporting – particularly when employing remote operation techniques – which are susceptible to manipulation. Such manipulation need not result in spectacular kinetic effects; the economic damage of shutting down e.g. a LNG liquefaction plant or a refinery for extensive overhaul and repair can be similarly dramatic, particularly when considering the effect of such an event on down-stream supply lines.

A discussion of the U.S. global critical energy infrastructure protection strategy was provided by Dr. Bruce Averill (Senior Coordinator for Critical Energy Infrastructure Protection, U.S. Department of State). Much of this centres on bilateral and multilateral cooperation, also involving commercial entities in activities such as training, technology assessments, and risk evaluation. It was also noted that NATO is as yet still investigating its own role in securing the energy infrastructure, as made evident by recent meetings.

Threats more specific to the Arabian Gulf region in the form of Chemical, Biological, and Radiological agents were discussed by Dr. Scott Savitz (Center for Naval Analysis, Alexandria, Virginia, USA). In the specific context of the Gulf, its fixed physical critical infrastructure and vessels traversing the area, biological and chemical threats are less likely to be a major concern since climate and weather conditions make it difficult for such agents to persist for a long time. Modern chemical warfare agents can persist for days under suitable conditions as are e.g. found in the cool climate of central Europe, but the high humidity, temperatures, and exposure to sunlight in the Gulf tends to degrade most such agents quickly; this also applies to biological warfare agents. Moreover, while it cannot be ruled out that biological or chemical agents will harm personnel and may have a severe impact on morale (e.g. leading staff to abandon their workplace for extended periods), the actual critical infrastructure is not harmed by the agent except indirectly.

While radiological agents can indeed persist for long times, their detection is also much easier to accomplish and can be done inexpensively with handheld and fixed devices; Dr. Savitz noted that the relevant procedures for protecting against such attacks had been the subject of successful exercises, particularly in the Kingdom of Bahrain. Moreover, once agents are detected, area infrastructure decontamination is a straightforward process as long as the necessary bulk chemicals are stockpiled in advance and wash-down facilities are available; beyond this, medical surveillance, the availability of treatments, and detection and inspection regimes can provide adequate protection.

A larger challenge is posed by the very nature of the energy infrastructure, particularly in the Gulf region as was

noted by CAPT A. Munem M. Al-Janahi of the Marine Emergency Mutual Aid Centre. Oil pollution both in the form of low-level spills and as a consequence of attacks has extremely severe consequences for the environment and also results in indirect consequences such as deleterious effects on the fishing and shipping industry and in some cases (when threatening the intake of power and desalination) also further impact on critical infrastructures.

The symposium also included a discussion of law enforcement aspects, particularly as related to information sharing among the different agencies and bodies in a complex multinational environment where the boundaries between law enforcement and national security are often fluid and must be reassessed frequently. To this end, Mr. Joseph Vann (U.S. Naval Criminal Investigative Service) presented the outline of an upcoming Maritime Law Enforcement Information Fusion exercise, Sea Falcon '08.

The challenges of securing the infrastructure in the Northern Arabian Gulf, particularly the oil delivery pipelines and trans-shipment terminals were highlighted by CDRE Allen du Toit (Commander, Combined Task Force 158, Combined Maritime Forces, Royal Australian Navy). Here, the combination of aging and poorly maintained physical critical infrastructure whose failure or destruction would have severe consequences for both the regional economy and also for the environment is further complicated by busy waterways and international borders, limiting the defensive perimeter. This requires good situational awareness throughout the entire Area of Operations, and a layered defensive structure that is capable of assessing and reacting to threats as they emerge.

The symposium was rounded out by two panel discussions, one on security aspects in which the issues of cooperation between governments, government-controlled and private sector infrastructure were stressed. In particular, the issue of translating policy statements on topics such as information sharing into operational doctrine were covered, as were the inevitable challenges of cultural and language differences, particularly in fluid environments where contingencies cannot always be prepared for exhaustively.

The second panel discussion dealt with issues of consequence management, once again with a strong focus on the oil and gas production and trans-shipment domain. While there was no immediate consensus on the likely severity of the conflagration or blast resulting from an attack on a LNG tanker (e.g. using an Exocet missile or even rocket-propelled grenades), the consequences of attacks on LPG or crude carriers are known and must be considered very severe. This also applies indirectly to Floating Production, Storage, and Offloading (FPSO) facilities that represent large and difficult-to-replace assets. One issue that was discussed in this context was the threat of mine deployment in restricted waterways; while the Gulf has had a history of mine warfare, and CTF 158 has accordingly deployed credible mine counter-measure assets, this will not necessarily be the case in other areas. In such cases the consequences may include not only the immediate damage to vessels and the environment (e.g. in case of crude oil carriers) but also the effects of blocking shipping lanes and also further indirect effects such as insurance costs and freight rates mentioned earlier.

The MIPS was attended by approximately 200 participants from more than 20 countries and included high-ranking representatives, heads of navies and chiefs of naval operations (or equivalents) as well as other government, industry, and academic experts.

Quo vadis? IT security as common task of state and economy

Marit Blattner-Zimmermann

Is a lawyer, based in Germany, with a lifelong career in the Ministry of the Interior. During the last ten years she has worked as a specialised manager on C(I)IP. Today she consults government and industry in C(I)IP issues.
E-mail: MaritBlattner@web.de

Introduction and actual situation

In less than a generation, information technology has successfully pressed ahead with its triumphant advance by pervading companies throughout the world.

Never before, frontiers have been collapsing as fast, never before the usual national structures have proven thus inefficient to solve challenges and problems as in today's IT networked world.

It can be assumed that the requirement of establishing IT security mechanisms to protect company interests has first emerged in globally acting companies. Confidential communication as well as integrity and availability have been recognised as indispensable elements of enterprise welfare.

Today, information and communication technologies (ICT) are central elements of our societies. States, economies and citizens use these technologies and profit from their advantages. With its growing spread in all spheres of our lives, new threats have arisen for the single user and for the society as a whole.

While in the past, e.g. secure cryptographic technologies were a privilege of government organisations to protect confidential or secret messages, today, it is especially sensitive enterprise information that requires commercially available, secure and user-friendly cryptographic protection.

Economic espionage and criminal activities in all thinkable variations have developed fast – much too fast – and new fields of activities related to and exploiting IT networks.

A black economy of organised crime increasingly harms enterprises as well as industrial nations. Especially the use of suitable and powerful cryptographic techniques can effectively limit data theft. Data integrity and authentication are essential for the dependability of business relations and its undisturbed processes, so that appropriate security solutions for integrity and authentication have been established in the market.

Procedures for electronic signature are almost globally available and ensure a justified trust of contract partners in e-commerce. Germany put an early sign with the first national electronic signature law. At a time when technical solutions have not yet been sufficiently advanced, Germany has recognised the chances for new types of secure business over open IT networks, and a remarkable gain in security for electronic commerce as well as for IT applications of the federal administration has been achieved. Several years later, national barriers have been overcome with the European guideline for electronic signatures, and the foundations of the complete electronic handling of business processes within the European Union have been laid.

Through fast spreading pictures and reports on internet and TV, the events of September 11 have dramatically shown to the world its vulnerability.

However, even power failures with impacts registered around the globe can, in case of insufficient security measures, lead to tremendous disadvantages up to insolvency or bankruptcy of the affected companies. Irrespective of the cause, be it terrorist violence, human error or forces of nature, an ICT-outage in an enterprise is under all circumstances a serious scenario which can at most be met by adequate BCP (Business Continuity Planning) and ICT security measures.

The availability of ICT is of central importance particularly for providers of critical infrastructures. Services that are essential for the survival of society, such as power and food supply, operational traffic and telecommunication services, must be ensured. The German critical infrastructure (KRITIS) community is aware of its specific responsibilities and has effectively established a multitude of ICT security measures and structures within its organisations.

Security Standards as a guide for IT security in companies

Nowadays, enterprises are in general set up well enough with human and material resources and an adequate organisation to manage their own ICT supported business processes in a reasonably secure way.

The truism that a chain only is as strong as its weakest link still proves true especially in the vulnerabilities that may arise from differing legal requirements, non-harmonised standards and missing international agreements. Several ISO standards provide guidelines and rules for ICT security that are outstandingly well qualified to shape enterprise organisations to achieve audit compliant as well as to provide a basis for corresponding ICT-security certifications.

In Germany, an ICT security agency specialised for all aspects related to ICT security, the Federal Office for Information Security (BSI), has already been established in 1991. Being a service provider for multiple target audiences, the BSI supports and advances the development of international standards, and releases as national standards and recommendations.

Thus, Germany could significantly contribute to the ISO standards for certification of ICT security products and ICT security procedures and was among the states that jointly developed European (ITSEC) and later international criteria for certification (CC). In the meantime, 24 nations have signed a mutual recognition agreement. This means that just one certifying procedure is today sufficient for developers of ICT security products and systems to obtain a certificate recognised in numerous countries.

BSI-standards provide recommendations of methods, processes, procedures and measures related to information security. With IT Grundschutz [1] (IT baseline protection), the BSI has considerably influenced international benchmarks for IT security. The BSI takes up topics that are of fundamental importance for information security in the public administration and enterprises as well as useful approaches established nationally and internationally.

At the same time the harmonisation of legal requirements towards companies' ICT security is urgent

Private businesses and the public administration can make use of the BSI recommendations and adapt them to their own requirements. Safe and secure use of ICT is supported because it is possible to resort to established methods, processes or procedures. Certainly, also developers of information technology as well as service providers have the possibility to take advantage of the BSI recommendations to enhance the security of their products and services.

In spite of intensive national efforts, the demand of globally harmonised technical requirements with respect to ICT security and ICT standards could not yet be sufficiently met. At the same time the harmonisation of legal requirements towards companies' ICT security is urgent and challenges the community of states due to quite diverse legal systems.

At least in Europe, first considerations of law harmonisation can be seen. The especially delicate fact is that already within one nation highly differing approaches and motivations for legal regulations may be found. National structures and diverse regulation and control authorities do not necessarily influence the ICT aspects of businesses in a sufficiently consistent way as different functions determine or have individual influence on law and regulations.

[1] http://www.bsi.bund.de/gshb/intl/index.htm

As a result it must be assumed that even a partial harmonisation of requirements will be a hard and lengthy process and that the problem of an court-proof ICT security organisation in businesses will be of increasingly importance not only due to liability limitations.

Legal consultants and chartered accountants cooperate with ICT and security specialists to commonly develop feasible solutions. In Germany, universities and independent law institutes equally deal with this broad field so that in spite of still numerous open questions enterprises have access to highly qualified advice.

ICT security as a government obligation

Security as duty of states, international co-operation, balancing of interests, civil interests and regulation requirements are several topics being closely related to ICT security.

The Federal Minister of the Interior is responsible for the national security in Germany. In 1991, the Federal Office for Information Security has been established to complement the already existing public agencies for national security, the Federal Criminal Police Office (BKA) and the Federal Office for the Protection of the Constitution (BfV). The objective of the legislator was to enable the timely detection of intrusions into information systems with criminal, extremist or intelligence motivations, the assessment of their effects and the demonstration of f evidence (Bt Drs. 11/7029). This was a consequent decision due to the increasing threat to ICT security, which established co-ordinated ICT security precautions also in the federal administration as an effective measure of prevention of hazards.

The merging of computer security and communication security as response to their fading differentiations as well as the subsequent orientation of the BSI towards economy and citizens are today a well-established contribution to offer

solutions against the risk due to the use of information and communication technologies.

An essential challenge for the BSI is to develop and propose technical and organisational measures to avoid or repair respectively disturbances or disruptions of ICT. Yet it is irrelevant whether the reason lies in human action or technical errors.

By establishing the Federal Office of Civil Protection and Disaster Assistance (BBK) after the terror attacks of September 11, the Federal Minister of the Interior (BMI) has expressed his responsibility for physical protection as well. Along with the traditional tasks for the protection of the population, the baseline protection concept describes both the reduction of the vulnerability of critical infrastructures through natural disasters and accidents as well as through terrorist attacks and criminal acts. (Schutz kritischer Infrastrukturen – Basisschutzkonzept, BMI, 08/05)

The Federal Government has expressed its responsibility for the security of services of critical infrastructure providers through fundamental concepts and implementation plans. The government thus underlined that the national security of Germany also focuses on ICT security.

At the chancellor summit in December 2006, the presence of politics in field of information technology was demonstrated in partnership with industry and business associations. This was underpinned at a European security conference held during the German presidency of the Council of the European Union in June 2007. The national and international German commitment to information security will thus provide contributions for secure and dependable use of ICT in all areas of economy and administration today and in the future.

Regulation and Partnership

Partnerships and similar forms of co-operation between responsible public authorities as well as the close co-operation between public administration and companies to promote increasing ICT-security in economic and administrative communication are essential. This is even more valid for the availability of secure and trustworthy products. Especially the big market leaders are responsible to consider the foundations of trust into the security of their products next to profit and market presence. It should not be necessary to stimulate the consumer demand for security by introducing additional regulations and legalisation.

For the modern information society to prosper it is essential that all participants of ICT processes take responsibility for ICT security.

As a result of the privatisation of formerly public sectors like the postal and the telecommunication services, supervising and regulation authorities like the Federal Network Agency (BnetzA) and others have been appointed in Germany to guarantee the service delivery by the effected companies in the interest of state and consumers. Consequently, German companies must comply with numerous obligations which are not equally relevant for all players in the international competition. For the service providers of critical infrastructures, it is of special interest to pursue the way of the least possible regulation in the field of ICT security.

Against this background, a culture of trust is not self-evident. While the state traditionally tries to apply means of regulation to fulfil to its best the task of ensuring the national security, economic players tend to perceive regulations more likely as impediment to competition and are sometimes inclined to ass me that the regulating authorities don't possess sufficient knowledge with respect to the true requirements within companies and markets.

It is time to change minds so that also in the future, it will be possible for state and economy to use the stable "platform Germany" in security and freedom.

National strategies

The Federal Government of Germany has realised this need and presented a common basis for the ICT security in the future. The national plan for protection of the information infrastructure (NPSI, BMI, 07/05) is the government's umbrella strategy for ICT security. Prevention, reaction and sustainability are the areas where measures for economy and administration commence to optimally protect ICT as the nervous system of Germany. The NPSI shall guarantee that the indispensable co-operative proceeding of state, economy and society in common responsibility but with distributed duties leads to the same ambitious destination.

A dedicated working party within the Federal Ministry of the Interior (BMI) controls and co-ordinates the activities to improve the protection of critical infrastructures and, thus, supports the concerted efforts of all participating groups. Within the scope of its line supervision the BMI IT staff supports and directs all activities of the BSI to secure the ICT in critical infrastructures.

The Federal Office for Civil Protection and Disaster Assistance (BBK), the Federal Criminal Police Office (BKA) and the Federal Agency for Technical Relief (THW) work on further aspects of infrastructure protection.

The other federal ministries and especially economy representatives are included continuously as well. The implementation plan KRITIS (UP KRITIS) as a sub-concept to realise the National Plan was drafted under intensive participation of affected companies. The actual state of ICT

security in the participating companies could be investigated and assessed. Recommendations are made and further steps are agreed upon cooperatively by all participants to adapt and enhance the protection of critical infrastructures to meet new and increasing challenges. The economy has an extraordinary responsibility in all these tasks. Roughly 85% of critical infrastructures in Germany are currently privately owned. The agreed cooperation between state and economy certainly contributes to the improvement of the protection of critical infrastructures. The state initiates and activates the work. It provides support and offers the competence of the BSI and its participation in working groups. The final responsibility for the application of adequate measures to guarantee the availability, confidentiality and integrity of the critical processes lies undoubtedly in the hands of the providers. The process of building trust and cooperatively assuming common responsibilities has started and is already producing first successes. It will continue to be the preferred way if all participants remain aware that the protection of critical infrastructures concerns all: state, economy and the citizens as users of the corresponding services. This way enables to bundle up narrow resources and offers new chances to optimize activities. The cooperation will also offer new ways of common research and development in the field of ICT security. Altogether, the partnership of state and economy offers a chance to minimize regulations and redefine activities based on a common understanding.

The glance to Europe

It is obvious that, next to numerous national approaches, the demand of the economy to find common solutions, standards and strategies must be considered in Europe as it overcomes differences and is growing together. The European Union has expressed its responsibility for this task by establishing the ENISA institution to co-ordinate national positions in the field of ICT security. Next to a green paper on the European Programme for Critical Infrastructure Protection and the European Programme for Critical Infrastructure Protection (EPCIP) itself the European commission supports national efforts in many fields like the establishment of Computer Emergency Response Team (CERT) structures or of international watch and warning projects.

With the 6th and 7th framework programme of the European Union, another contribution is made for common research and development in this field throughout Europe.

The realisation that purely national efforts will hardly be sufficient to guarantee in future for the required degree of ICT security in Europe for member states as well as for economies and societies allies and unites us all. Still remaining and sometimes contradictory positions will of course have to be discussed. At the end, nobody shall close himself off from the fact that future challenges for industrial nations can only be met concertedly. The fields of information technology and its security can not be excluded.

Outlook (Wish and Reality)

Due to different approaches that are not generally compatible enterprises face challenges that can be met a lot easier if the political support can be optimised and accelerated nationally and internationally. The desire for market solutions for all ICT security problems, the demand of standardised and possibly worldwide valid legal requirements and the hope for globally equally goal-oriented measures of legislation and government remains still a vision of a not yet evident future.

The way towards the right direction is therefore long, but not only in Germany but in other countries as well it is already adopted.

2030: IT Security – quo vadis?

Specialised attacks of organised crime and terrorists on ICT processes of large trusts are handled as cyberwar by the international state community. Netiquettes for the behaviour in the Internet and all modern communication networks exist in all nations. International agreements allow for the persecution of offenders across national boundaries without any delay. Legal norms for the required level of ICT security in companies to protect business processes have been standardised. Financial supervision, chartered accountants and persons in charge for security apply the same harmonised legal standards for the assessment of ICT security in companies. There are insurance companies that offer insurances against the few remaining contingency risk factors of ICT at reasonable rates.

The use of certified ICT products and systems in critical processes is already self-evident. There is a sufficient spectrum of protection profiles for such processes. Almost all providers offering relevant supply services are certified related with respect to ICT baseline protection.

As a matter of course adequate and sufficient resources for ICT security are allocated in financial planning of all organisations. In every company with more than 100 employees there is not only a person responsible for ICT but also an expert for ICT security.

The demand for external ICT security revisions is enormous as by proving that the revision results have been put into action insurance rates and financial reserves can be considerably reduced.

State and economy work trustfully hand in hand to further develop the advantages of modern information technologies and avert disturbances of any kind in advance.

And we all can take part in this development!

A Look at Approaches to Risk in the United States

The recent publication of a monograph on critical infrastructure protection and risk lends to enhanced knowledge of risk in the homeland security context

Elizabeth M. Jackson

Senior Associate, Special Projects Critical Infrastructure Protection Program
George Mason University School of Law

e-mail: Ejackso4@gmu.edu
http://cipp.gmu.edu/

Countries around the globe have long been concerned with issues of protecting critical systems, assets, and networks to ensure the provision of essential services and maintain national security, economic stability, and public health. The United States has been particularly cognizant of the need for critical infrastructure protection (CIP) and recently moved towards a more focused, risk-informed approach to CIP. Risk is not a new concept; gauging risk as part of a cost-benefit analysis for the insurance industry, as a means of judging the vulnerability to failure of a new government initiative, and to guide decision-making with regard to the assignment of law enforcement officers to particular parts of a large city are merely a few examples of its use. Only in the past decade or so has risk taken such a prominent role in homeland security.

Given the increasing use of the term *risk* in discussions on homeland security and CIP, attention must be paid to ensuring there is a common understanding of risk and the elements that comprise risk. Moreover, knowledge of how risk is assessed and how it is managed on various levels, such as strategic or operational, is key to better informing decision-makers and enhancing overall risk management efforts. Thus, in an effort to promote a greater understanding of risk, the George Mason University School of Law's Critical Infrastructure Protection Program published a monograph entitled *Critical Infrastructure Protection: Elements of Risk* in December 2007.

Risk is not a new concept . . . but . . . Only in the past decade or so has risk taken such a prominent role in homeland security

Risk Assessment vs. Risk Management

Given the many applications of risk, terminology used in discussing this topic may vary. Simply put, and as asserted by numerous authors within the monograph, there is no common lexicon for risk. Typically, this does not pose a significant problem for practitioners, as discussion content is understood regardless of the specific words used to describe the many elements or variables of risk. However, those who are not subject-matter experts, most often senior decision-makers who serve as end-users of risk assessments, frequently encounter difficulty in truly understanding what risk is and what information will be gleaned from a risk assessment. A lexicon for risk analysis will assist decision-makers in the comprehension of basic concepts of risk and the differences between risk assessment and risk management, as well as what can be expected of each.

Differentiating Risk Assessment from Risk Management

Risk Assessment

Despite variations in terminology, the standard formula for risk in the homeland

security context remains constant, where risk is described as a combination of threat, vulnerability, and consequence. Risk assessment addresses the following questions:

- What can happen? In other words, what is the range of plausible hazards that threaten critical infrastructure?
- How likely are these hazards to occur? In other words, what is the potential for these hazards to occur and inflict damage on critical infrastructure?
- What are the consequences if they do occur?

An *actionable* risk assessment moves beyond these questions to offer suggestions for how the variables of risk can be influenced to achieve favorable benefits in terms of risk reductions (i.e., mitigate risk), as well as information on the nature of the risks facing the decision-maker.

Risk Management

Risk management involves the consideration and implementation of measures to reduce the challenges identified in a risk assessment. It seeks to answer the following questions:

- What are my options for identifying, controlling, and mitigating – or buying down – risk?
- What are the trade-offs in terms of costs and benefits for each option?
- What impact will these options have on my future risk reduction efforts?

Understanding the above differences between risk assessment and risk management enables decision-makers to look past the terminology and review relevant information to assist in their decision-making processes. With a basic understanding of risk and what feeds into the management of risk, lines of communication are enhanced between key stakeholders at varying levels.

A Focus on Risk in the United States

To further frame the discussion, the following definitions from the U.S. Department of Homeland Security's National Infrastructure Protection Plan (NIPP) are noted:

Risk – a measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the NIPP, risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.

Risk Management Framework – A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.[1]

Understanding the differences between risk assessment and risk management enables decision-makers to look past the terminology

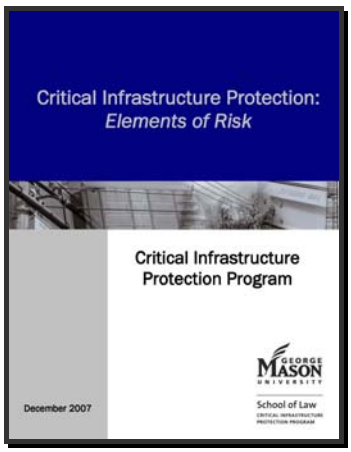
The NIPP was drafted in response to a congressional mandate in the Homeland Security Act of 2002, specifically that the Department develop a "comprehensive national plan for securing the key resources and critical infrastructures in the United States,"[2] and additional requirements put forth in Homeland Security Presidential Directive (HSPD)-7: Critical Infrastructure Identification, Prioritization, and Protection. It also built on elements of the National Strategy for Homeland Security, first released by the Executive Office of the President in July 2002. The completed NIPP, released in June 2006, reflects a greater emphasis on risk than the preceding Interim NIPP and was considered by the Department a "comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies and tribal partners."[3] Since the release of the NIPP, the Department has continually placed an emphasis on risk-based approaches to better protecting the Nation's infrastructure from all hazards.

Notably, although the threat of terrorism remains on the minds of U.S. leaders, the population and infrastructure of the United States are more susceptible to negative impact by accidents and natural disasters than terrorism as it is commonly defined. Regardless of the type of threat, risk assessments can be performed to contribute to the management of risk and better informed, hence improved, decision-making. The CIP Program's monograph on CIP and risk presents information that can be applied to risk in any case, and gives particular attention to vulnerability, arguably the most important variable of the risk equation.

Risk Monograph in Brief

The papers included in *Critical Infrastructure Protection: Elements of Risk*, generally referred to as the risk monograph, address numerous topics related to risk, including the definition of risk, assessment methodologies, and strategic approaches to risk management. They offer suggestions for improved risk management, information on current practices as examples of risk-related efforts underway in the United States, and allude to continued growth in this challenging and dynamic field. The monograph does not include papers delving into specific sectors, nor is it meant to endorse any one methodology or

technology used in assessing and managing risk.



The seven papers that constitute the risk monograph are summarized below in the order of presentation.

In *Security Risk Management: Implementing a National Framework for Success in the Post-9/11 World*, Edward Jopeck and Kerry Thomas of the Security Analysis and Risk Management Association (SARMA) acknowledge an all-to-common gap between the information sought by policy makers and the information practitioners can produce to meet what policy demands. The authors review progress made since the September 11th terrorist attacks with regard to security analysis and risk management programs in the United States. They also discuss the importance of a national strategy for security risk management and detail recommendations for improving security risk management processes.

Geoffrey French of CENTRA Technology, Inc. explores the first variable of risk, threat, in *Intelligence Analysis for Strategic Risk Assessments*. He notes the need to expand on the traditional nature of the U.S. Intelligence Community to better allow it to assess threat and mitigate risk. Specifically, the author asserts that evidence-based threat assessments and imagination-based analysis should be performed when conducting strategic risk assessments. Elaborating on the necessary ability to adapt to changing needs, French reviews shifts within the Intelligence Community, as well as current advantages and disadvantages of numerous types of threat analyses.

Turning further towards the technical side of assessing risk, information on vulnerability, vulnerability assessment, and the use of network modeling to aid in risk management is presented in the next three papers:

In *The Meaning of Vulnerability in the Context of Critical Infrastructure Protection*, William McGill and Bilal Ayyub of the University of Maryland define vulnerability as it relates to CIP and describe overall vulnerability in terms of two general categories, protection vulnerability and response vulnerability. For each category, the authors offer mathematical expressions to measure vulnerability, taking into account probability of threat events occurring and the consequences of exploitation of vulnerabilities. They also address specific security considerations that must be taken into account when assessing vulnerability, thus enabling greater risk mitigation.

In *Vulnerability Assessment of Arizona's Critical Infrastructure*, Todd White of the Phoenix (Arizona) Police Department / Arizona Counter Terrorism Information Center and Samuel Ariaratnam and Kraig Knutson of Arizona State University offer an example of state government CIP activities through a discussion of the State of Arizona's terrorism prevention program. The authors provide information on projects developed to educate first responders and government officials in protection systems, assist in the prioritization of infrastructures, aid in the performance of threat and vulnerability assessments, and improve site design and design standards. In doing so, White, Ariaratnam, and Knutson address topics such as data collection, site evaluation criteria, and protective design measures.

Thomas Mackin of California Polytechnic State University and Rudy Darken and Ted Lewis of the Naval Postgraduate School explore the use of network analysis as part of a risk-based approach to CIP in *Managing Risk in Critical Infrastructures Using Network Modeling*. The authors detail the critical node analysis technique and outcomes that can be expected from its application to diverse infrastructure. Such outcomes include determinations of criticality, valuable information for use in the allocation of resources, and development of fault trees. To articulate its efficacy in calculating and managing risk, Mackin, Darken, and Lewis provide an example of critical node analysis applied to a petroleum transmission system.

Same Words, Different Meanings: The Need for Uniformity of Language and Lexicon in Security Analysis and Risk Management by Andrew Harter, formerly of SRA International, Inc., offers strategic food-for-thought by way of a review of the need for a common lexicon in the field of security analysis and risk management. The author asserts that confusion over terminology can impede decision-making and reduce the effectiveness of risk management efforts. Accordingly, to assist key stakeholders in managing risk, Harter advocates the development of voluntary consensus standards. In explaining the process of standardization, the author provides a case study of the SARMA Common Lexicon Project.

In the final paper, *The Intangible Value of Security in a Volatile Global Economy*, Robert Liscouski of Centurion Holdings, LLC and Nir Kossovsky of Steel City Re, LLC address the need for consideration of security risk in corporate business practices. The authors argue that intangible asset value is vulnerable and note that an increasing number of companies are discussing terrorism risk figures in the boardroom. Taking into account the linkages between security and enterprise value, they recommend the

development of good security risk management practices to ensure the protection and resilience of corporate activity. Referencing the work of the Intangible Asset Finance Society's Security Risk Management Committee, Liscouski and Kossovsky describe five steps, ranging from identifying priorities to battling complacency, that stakeholders – or shareholders – should follow with regard to security risk management.

Critical Infrastructure Protection Program Background

The CIP Program is a research entity dedicated to exploring topics related to CIP and spurring discussion of key issues among stakeholders in the critical infrastructure community, from Federal, State, and local government representatives to private sector owners and operators to academia and others with a vested interest in critical infrastructure. The Program's mission is to:

- Integrate basic and applied research in the disciplines of law, policy, and technology;
- Perform timely and focused analysis of current issues;
- Convene critical communities for action; and
- Conduct outreach and awareness for key decision-makers and stakeholders.

To fulfill this mission, the CIP Program serves as a valuable multi-institutional resource for providing innovative, original research; serves as a national forum for exploring concepts and developing real-world solutions for protecting the Nation's critical infrastructure and key resources (CI/KR); and enhances preparedness, protection, and resilience of critical infrastructure by performing analyses and advising on key CIP issues and research trends, leading scholarly discussion, promoting industry awareness, and supporting public-private partnerships and initiatives.

In bringing together the voices of practitioners in various areas of homeland security and CIP, the CIP Program contributes to broader discussions on important issues facing both the United States and international entities, whether nation-states or partnership organizations. The development of monographs in addition to research staff-authored white papers, discussion papers, and other products has also been instrumental in enhancing public awareness of critical infrastructure and homeland security subject-matter.

In bringing together the voices of practitioners in various areas of homeland security and CIP, the CIP Program contributes to broader discussions on important issues

The risk monograph can be accessed at http://cipp.gmu.edu/research/CIP_Risk_Monograph.php. Additional projects related to risk are underway, including the publication of a paper on regional (multi-jurisdictional) risk assessment and co-hosting of SARMA's conference on security analysis and risk management in May 2008, www.sarma.org .

Please visit http://cipp.gmu.edu/ for further information on the CIP Program and its work with respect to the numerous facets of critical infrastructure protection. The Program's website features a wealth of information on CIP; select research products and issues of its monthly newsletter, *The CIP Report*, are also available for download.

The author would like to thank William McGill for his invaluable input, and for allowing her to leverage his well-respected expertise in the area of risk.

[1] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, June 2006, p. 105.

[2] Homeland Security Act, §201. H.R. 5005, 107th Congress/2nd Session, Public Law 107-296, November 25, 2002.

[3] U.S. Department of Homeland Security, "DHS Completes National Infrastructure Protection Plan," Press Release, June 30, 2006.

.

Cyber Security of Control Systems.

All those involved in control systems have a part to play in helping to meet the security challenges we face today. This article outlines the challenges and what can be done to meet these challenges with solutions.

Karl Williams

Principal Consultant at Invensys Process Systems and responsible for security services in Europe, Middle East & Africa. CISSP and IISP.

E-Mail: karl.williams@ips.invensys.com
www.invensys.com

Understanding the challenges

Control systems have seen a great deal of change in recent times, including increasing connectivity and the use of open standards and protocols from a previously proprietary and often isolated environment. This use of "off the shelf" technology driven by requirements for additional applications, analysis and operational visibility, combined with connectivity to business and other networks brings great benefits such as interoperability and efficiency, but also creates challenges for security.

Karl Williams is speaks at the IIR SCADA conference June 16/17, 2008 in Stuttgart, Germany: www.it-produktionssicherheit.de/

The security threats and vulnerabilities we see today are wide ranging and often complex and are not always well understood, particularly what impact if any they may have on an individual system or facility. Threats come from a range of internal sources such as removable media, as well as from external sources such as connections with other devices and networks. Threats can change quickly as new vulnerabilities emerge, meaning that control systems may find their normal operation impacted simply because they share, either directly or indirectly, a technology or connection. While this impact may not necessarily be directly disruptive to the plant it may reduce efficacy and that in itself is undesirable. In addition there may be compliance or regulation to address depending on the industry.

Effective policy, procedures and enforcement (assessment/audit/monitoring) is crucial for safe and reliable operation.

The good news for all those involved, including system owners, operators, vendors, consultants and suppliers, is that by working together to understand, manage and reduce security risks we can maintain the critical services that we all rely on.

Meeting the challenges

To face the challenge, involvement in activities across the control systems industry is a prerequisite, as e.g. participating in industry security standards groups and information sharing activities, such as ISA99 http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821, ISCI (ISA Security Compliance Institute) http://www.isa.org/Content/NavigationMenu/Technical_Information/ASCI/ISCI/ISCI_History.htm, Process Control Systems Forum (PCSF) https://www.pcsforum.org/ as well as other groups. These groups provide the opportunity for greater understanding, knowledge transfer and sharing of expertise and information. In addition, many countries now have Critical National Infrastructure initiatives initiated by governments and organise conferences; e.g. "Global Government Critical Infrastructure Protection" Meridian 2007 conference in Stockholm http://www.meridianprocess.org/ facilitated by the Swedish Emergency Management Agency www.krisberedskapsmyndigheten.se .

With such a wide diversity of control systems deployed from the most up to date to those that are much older, there is a need for differing security measures; the risk faced by the newest systems is often different to that faced

by older (legacy) systems, nevertheless the security position still needs to be understood and security for all systems needs to be effective while allowing critical functions to be performed when required.

Providing more secure products that includes host based firewall, hardening of workstations, anti-virus and vulnerability testing all contributes to lowering the risk of a security incident. While putting in place mitigation measures will initially improve security, the on-going management of security technology needs to be considered to maintain this position. So, whether the expertise is internal to a control system user or there is a need to bring in external expertise, solutions are available, e.g. Invensys has addressed this element by recently establishing a partnership with Integralis, a leading security management service provider. Using external expertise provides a range of benefits to help with quickly changing threats and vulnerabilities.

Security solutions

Security based on best practices will be more effective, e.g. Invensys uses the following principles:

- View security from both management and technical perspectives
- Ensure security is addressed from both an IT and Control System perspective
- Design and develop multiple layers of network, system and application security
- Ensure industry, regulatory and international standards are taken into account
- Prevention is critical in plant Control Systems, supported by detection

Layered Security – defence in depth

Defence in depth approaches are recommended for designing and implementing measures to mitigate security vulnerabilities and threats. The diagram (Fig. 1) shows an example of a typical architecture used to address a range of security risks.

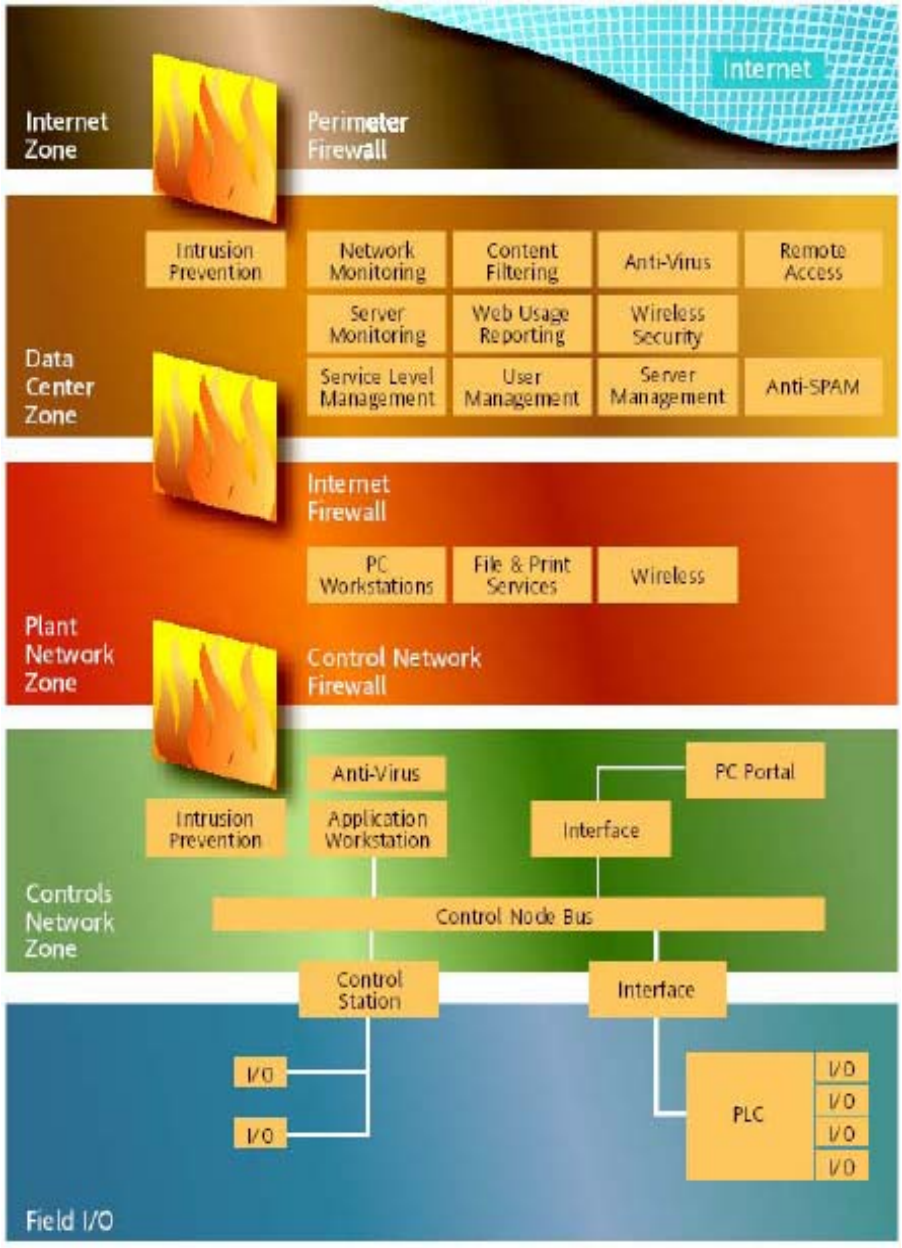


Fig. 1: Layered Security

Each layer is evaluated for its criticality and corresponding risk and appropriate security measures applied. To proceed through each layer a security threat must compromise each security measure, both management (polices and procedures) and technical: this approach creates a more resilient architecture.

The selected approach ensures that the most critical assets receive the greatest layers of protection; threats are more likely to get a timely response.

This defence in depth strategy, when successfully implemented and managed, minimises the likelihood of a threat being successful and provides intrusion prevention; these security measure are effective and proactive.

A cyber security program should meet the individual requirements of a particular user, system and site. In general a cyber security program should be emphasis the following topics:

- Security Assessment;
- Security policies, procedures and enforcement;
- Protection with appropriate technology;
- Security training for knowledge transfer;
- Security management.

Security Assessment

A security assessment is one of the first steps in developing and understanding the security position of a control system. The results of an assessment are the base on which an appropriate security approach can be defined.

Security Policy, Procedures and Enforcement

Effective policy, procedures and enforcement (assessment/audit/monitoring) is crucial for safe and reliable operation. The development of policy and the supporting procedures is user and facility specific and should therefore be developed in close cooperation with the system users to ensure the result is workable and effective. Management support at all levels in this area is vital to ensure success of such security projects. Any corporate/business policy and procedure requirements should be taken into consideration during development.

Protection with technology

Technology plays an important part in the overall security approach. Firewalls are just one example of a technology that provides part of a defence-in-depth design and when implemented and managed correctly can mitigate security vulnerabilities and threats. Design and implementation of an architecture using a DMZ provides more secure access and control; by including additional features such as anti-virus and deep packet inspection there is additional protection. The on-going management of firewalls and other devices should be carefully considered as well.

Invensys currently provides its control system workstations pre-installed with Anti-virus (AV) software and a host based firewall. The effectiveness of AV must be maintained with regular updates; an out of date AV product gives no protection against new malicious code. A suitable update method should be in place for systems both with and without network connectivity; this will give protection against viruses that may be brought into a system by removable media such as USB drives or CD.

By working together to understand, manage and reduce security risks we can maintain the critical services that we all rely on.

Training for knowledge transfer

Those who have access to a control system, either directly or indirectly, frequently or just occasionally require appropriate security training to ensure low risk. Training is essential in ensuring coincidence of interaction with critical systems and its useful or harmful impact. Training is needed to enable those involved with operational systems to understand the policy, procedures, enforcement and the wider security picture. Training should emphasis technical aspects as well, such as Firewalls, Intrusion Detection & Prevention and AV updates.

Security management

The umbrella security management may unite many activities like safety programs that are in place. Safety in this context is a daily way of life, continuously monitored, validated and well understood. cyber security management will require the same approach and adaptation.

While there are some security elements that are rarely updated once in place such as policy, other parts will need more frequent or even continuous attention such as AV updates, firewall management, business continuity. Each system will need to be assessed for its own need based on its circumstances, but following a continuous life-cycle model of Assess, Design, Implement and Manage, with supporting elements in each phase provides the flexibility needed for a low security risk environment.

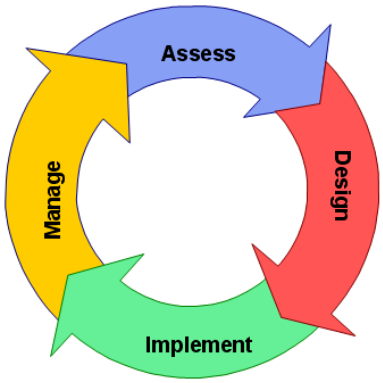


Fig. 2: Security Management Cycle

Convergent and Cross-Sector Risk Trends for Security and Continuity.

The author describes from the viewpoint of a CNI company the changing threat profile of production systems and the requirement to collaborate across sectors and countries to prepare against the growing risk

Michael Freiberg

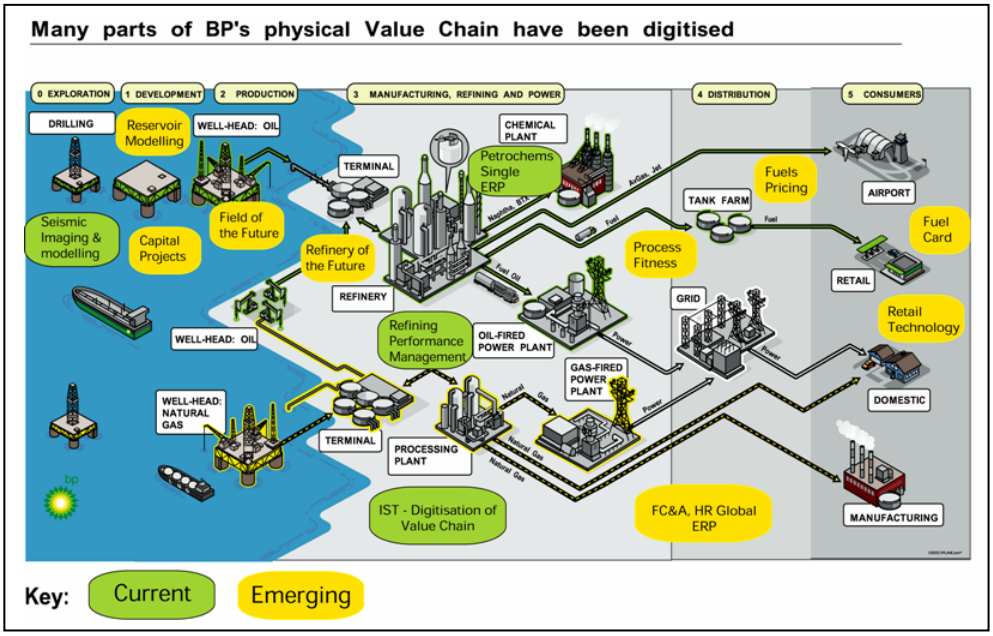
Security Consultant to BP Plc. & Acris GmbH
Head of German UP KRITIS Working Group 1
CISM, IISP Assoc
e-mail: Michael.Freiberg@acris.ch

The German Federal Office for Information Security and Dr. Markus Dürig, Head of Division IT 3 – Information Technology Security at the Federal Ministry of the Interior (our Homeland Office) had asked me to present on CeBIT's Public Sector Parc about the motivation to support the initiatives around Critical National Infrastructure (CNI) and Critical national IT Infrastructure.

This led to the invitation to write an article, so that the content reaches the readers of this newsletter.

cations which support the physical workflow of BP, an example of a major player in the oil industry:

Now you could say: "welcome to the club, what's new?" So far most of the sectors with high IT dependency are at risk not to deliver their IT based services – which in itself is bad enough -, but there is relatively little knock on effect to be worried about. Now we live in a world where terrorists have used mobile – computerised – phones to trigger bomb explosions and unfortunately enough all



Whereas telecommunication and banking have a high dependency on IT infrastructure availability, the Oil and Energy firms still seem to have limited IT dependence. This perception is increasingly proving wrong; here is a pictorial view of appli-

production places in the above picture are handling explosive goods. Therefore, it could be an extremely powerful scenario to blackmail or attack production places through IT infrastructure or applications.

The possibility of such threats led to the conclusion that physical and digital Security as well as Business Continuity and Crisis Management need much closer interaction, because a malicious software or individual does not care how a company or a sector is organized, probably weaknesses in the way how processes are set up increase the impact of an attack quiet significantly.

Therefore BP Enterprise Security & impact of an attack quiet significantly. Continuity (ES&C) is now established as a community of practice to provide a holistic risk management to businesses.

For ES&C there are some clear risk trends, which are worth to be shared, because if public and private sectors are not joint up to protect against these trends the likelihood of a major crisis is much more likely to happen:

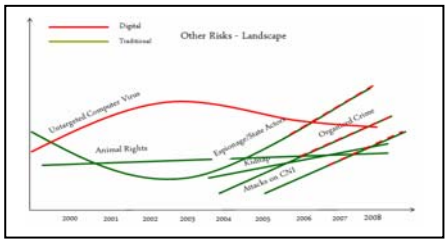


Figure 1: Perceived risk trends in BP Plc.

You can see that all the growing risk trends, is it espionage, organised crime or attacks on critical infrastructure will in our view have a very much blended nature, which could mean using physical means to attack IT infrastructure or applications or using digital means to attack physical infrastructure. Examples of such incidents are becoming plentiful:

- In 2000 a hacker attacked a waste water control system releasing millions of gallons of sewage into a hotel grounds and local river.
- In 2003 a nuclear power station safety system was infected by a worm which slowed down the control systems.
- In 2006 there were reports of hackers attacking control systems for profit.
- In late 2006, hackers gained access to the computer systems at a Harrisburg, Pennsylvania, water treatment plant. The FBI has investigated the incident and believes the attackers were working outside the U.S.
- In 2006 and 2008 representatives of the Intelligence Community confirmed to senior government and industry representatives that multiple critical infrastructure organizations had been penetrated and threatened with major outages if extortion money was withheld.
- In recent terrorist raids, computers and manuals were discovered to contain extensive information relating to SCADA and DCS vulnerabilities in dams and related structures especially the digital devices involved in these systems were seized.

There is a wide variety of incidents reported to researchers in this field.

- Denial of service typically resulting in one of two main consequences: Loss of view of the plant (i.e. the operator is not able to monitor what is happening on the plant) or loss of control of the plant (i.e. the operator is not able to influence the operation of the plant).
- Unauthorized control, where an unauthorised party gains control of the all or part of the plant. This can have disastrous consequences.
- Loss of integrity, where the information reported to the control system operator is incorrect as a result of a security incident.
- Loss of confidentiality for example reputation considerations (e.g. a nuclear power plant with a protest group gaining access to the reactor's control system)

The following diagram demonstrates the growing trend. Unfortunately there is a serious shortage of data from the process control world as there are no formal bodies collecting this information and many organisations are unwilling or organisationally unable to report information on incidents.

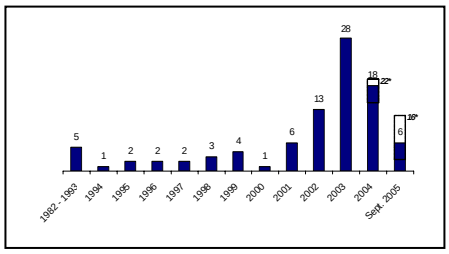


Figure2: Security Incidents in industrial control systems (Source: Who turned out the lights - Eric Byres, David Leversage, Justin Lowe – CSI 32nd Computer Security Conference & Exhibition)

The impact of such scenarios is not limited to a company or a sector; therefore it is in our best interest to support the KRITIS (Kritische IT Infrastrukturen) initiative initiated by the German Homeland office, which is laid out as a Public Private Partnership.

Currently two working groups are active, one dealing with crisis scenarios and an emergency exercises the other one with setting up warning, alert and crisis communication processes.

For a company working across borders it is vital that such initiatives take place in most if not all countries it operates, because many goods and services are not country bound, so cross country knock on effects are likely to happen.

In classic risk management terms you rank your risks according to a high/ medium/ low impact and vulnerability pattern (Some use more granular grids, but this does not change the principle).

In a next step one searches for "quick wins" by separating into "under control" "within influence" or "outside control" (or terminology with similar meaning). This is efficient use of time and resources and reduces the risk exposure fast and effectively – but only to a degree. By treating "outside control" as fate we produce an Achilles heel to our economy and the foundation of our society. We can push the outside control area quite a bit if we start to collaborate, protect and prevent across companies, sectors and countries. Only through such initiatives we can tame the coming risk trends not to become larger than live.

Managing security risk in industrial process control, automation and SCADA systems.

Process control systems have become interconnected and are now threatened by a growing number of security risk. The article gives technical background information to this risk and offers a good practice example how to manage process control security

Justin Lowe

Justin is a Managing Consultant with PA Consulting Group. He lead's PA's Industrial Cyber Security services and specialises in the security of industrial process control.
e-mail: justin.lowe@uk.bp.com

Ian Henderson

Ian in one of the small number of distinguished advisors BP has with the remit for Process Control Systems. For many years he worked as a Process Control engineer in Scotland.
e-mail: ian.henderson@uk.bp.com

Summary

Industrial process control, automation and supervisory control and data acquisition (SCADA) systems are commonplace to operate oil and gas, electricity systems, transport systems and manufacturing plants and often form part of a company's or even a nations critical infrastructure.

These mission and safety critical systems are at risk from electronic attack such as from hackers, viruses and worms because of the increased use of standard ICT like Windows, TCP/IP, web technologies and wireless. Such technologies have introduced security risk into an organisations control and operations environment that if left unmanaged, can cause significant business disruption were they to come to fruition.

In a changing and complex world companies such as electricity generation, transmission and distribution, oil and gas organisations are faced with potential interruptions that if not pre-empted and properly mitigated upon occurrence could cause severe interruption. These disruptions can carry a high price tag, not just in terms of direct financial losses but through loss of reputation or inability to fulfil commitments. It is essential that organisations assess their current protection against electronic threats and are prepared to respond to threats in order to minimise the threats to their own organisations and also to the critical national infrastructure.

These risk factors are relevant to all organisations which rely on industrial process control, automation and SCADA systems for the safe and reliable operation of their plant and processes. Industrial control system incidents are occurring but are rarely publicly acknowledged. The consequences of security incidents in these systems could have serious health, safety, environmental and reputation implications.

A recent increase in hacker attention on these control systems from years passed should raise the level of attentiveness for organisations at risk and implement effective protection measures and response processes commensurate with the business risk.

A pragmatic good practice framework has been developed from experience gained over the last five years in helping organisations address these risk factors, which is described in the last sections of this article.

Such technologies have introduced security risks into an organisations control and operations environment that if left unmanaged, can cause significant business disruption

Industrial process control is at risk of electronic attack

Industrial control systems exist in many forms and are often given different names such as:

- Process Control;
- Industrial Automation;
- Energy Management;
- SCADA;

- Telemetry.

Historically, process control systems were designed and constructed using proprietary technologies and installed in isolation from corporate IT-systems. However, recent trends include basing newer systems on more cost-effective platforms such as Intel or Windows. Moreover, the desire for remote control and management information has led to the adoption of common network protocols and the connection of many of these systems to the corporate IT network.

Whilst these changes have yielded many business benefits, it has also meant that control systems increasingly possess the same security vulnerabilities as corporate IT systems. Unfortunately, while these technologies have been adopted, the security protection measures that are usually found in the corporate ICT world have not been incorporated into control systems. Often these are for very good reasons. For example, a problem with a security patch can be life threatening in a control system. Also anti-virus software has an overhead in terms of operation and performance. This might not be a problem in a 'normal' IT system but this can have a serious impact in a real time control system.

Industrial control systems are not usually managed and protected by the corporate ICT department – they are usually maintained by engineering and operations teams who don't possess generally the ICT and security skills to protect these systems. Consequently many such systems remain vulnerable to electronic attack.

These vulnerable systems are increasingly exposed to external threats

For decades industrial control systems have formed part of the critical infrastructure for various countries and are mission critical for the process industries and manufacturing sector and have been designed for reliability and stability. Historically these systems were isolated from other systems and networks and therefore weren't exposed to significant security threats therefore security was not a big issue and consequently it was rarely built into their design.

In recent years there has been a drive to increase the level of management information from these systems, reduce operating costs and optimise production processes. This has proved a major driver for the connection of these critical systems to other networks and systems often introducing a path - albeit an indirect one - to the Internet and its associated threats.

All these connections expose these vulnerable mission and safety critical systems to a wider external world.

The wider world is increasingly hostile

Over the last decade there has been a dramatic increase in the number of vulnerabilities identified in software systems and consequently also the number of security incidents. Figure 1 shows a graph of vulnerabilities and incidents that have occurred during this time period in a wide variety of IT systems. Overlaid on this graph are a number of significant security events all of which have impacted industrial control systems.

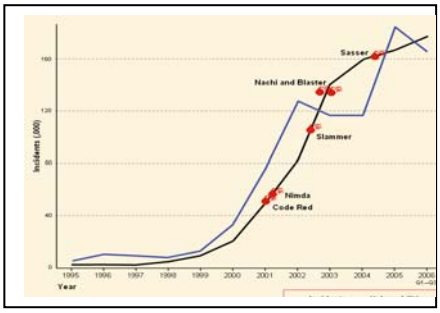


Figure 1 - Recent vulnerability and incident trends (Source: US Cert - http://www.cert.org)

Although this data covers all IT systems there has been a similar increase in incidents in the industrial control system world - see Figure 2, Michael Freiberg, Convergent and Cross-Sector Risk Trends for Security and Continuity, this issue of ECN. This article also lists some recent key incident in the process control arena. These data do highlight a significant increase in the number of industrial control system security incidents since 2001. There may be a number of reasons for this, specifically the increased use of windows and industrial Ethernet on the plant floor.

Over the past few years there has been an increase in control system related vulnerabilities and exploits in the hacking community, for example in 2007 at the Tourcon7 greyhat conference, where a security consultant gave a detailed breakdown on SCADA communication protocols and how to exploit them. More recently there have been reports of extortion threats involving industrial control systems. In addition there is evidence that organised crime is involved.

It is unlikely that these threats will reduce in the short to mid term so it falls to the owners and operators of these systems to provide protect these systems appropriately.

When considering the impacts of a security incident many people focus on the financial consequences of loss of production or operation. However in many cases other real life impacts can be far more significant. These can include damage to plant, environmental damage, non compliance with legal and regulatory requirements, health and safety or loss of license to operate.

A recent study by showed that around half of control system incidents resulted from an attack through the corporate network. While some companies have segregated control systems from corporate networks there are numerous repor-

ted incidents where hackers and worms have got through or around this protection to the vulnerable control system inside. This study also estimated the average cost of a control system incident at $1.8M (€1.4M). Where incidents resulted from a specific targeted attack, the consequences were significantly more severe, and could cost more than $10M.

Information about industrial cyber security incidents is generally under-reported. In many cases, the organisations themselves do not even know the extent of these incidents as there are few formal methods for collecting this information.

Managing the industrial control system risk

Organisations reliant on industrial control systems need to assess the risks facing these systems and mitigate this risk using appropriate protection measures. The author has assisted a number of major companies in the oil, gas and chemicals business for a number of years to address these risk factors and developed an effective Process Control Security framework which has been proven in practice and has been used to improve industrial control system security at a number of organisations. It also forms the basis of the guidance provided by the UK Government's Centre for Protection of National Infrastructure http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx .

Understanding business risk is key, their systems, vulnerabilities as well as possible threats.

Understand the Business Risk

All industrial control security improvements should be based on the business risk. Organisations should undertake a formal risk assessment with the following steps:

- Understand systems
- Understand threats
- Understand impact
- Understand vulnerabilities

Implement Secure Architecture

Once the business risk is understood, a coherent set of risk reduction measures must be implemented to form an overall secure architecture for the system.

In this context the term 'architecture' is used in the wider sense to cover the human elements of the systems as well as the technologies. A secure architecture will consist of a variety of process, procedural and managerial protection measures.

The risk management of Control Systems has to be holistic.

Establish Response Capabilities

The objective of this stage is to establish procedures necessary to monitor, evaluate and take appropriate action in response to a variety of cyber security events.

Establishing formal response plans and procedures ensures that any changes to the risk profile are identified as early as possible and any required response actions are embarked on quickly to avoid incidents or at least minimise the impact of incidents.

Improve Awareness & Skills

The objective of this stage is to increase process control security awareness throughout the organisation and to ensure that all personnel have the appropriate knowledge and skills required to fulfil their role.

Manage Third Party Risks

The objective of this stage is to ensure that all security risks from vendors, support organisations and other third parties are managed requiring:

- Identification of Third Parties - including vendors and service providers, and all other links in the supply chain, that are associated with the process control systems;
- Management of Vendor Risk - including procurement contract security clauses, ongoing vendor engagement, provision of security guidance, operation of security processes, effective software patching processes, vendor system hardening procedures, audits;
- Management of Risk from Support Organisations - including risk assessments and countermeasures, access control, support organisation engagement and awareness;
- Management of Supply Chain Risk - including engagement with any organisation in the supply chain to provide assurance that their risk is adequately managed. Examples of such organisations might include: suppliers, distributors, manufacturers, or customers.

Engage Projects

The purpose of project engagement is to ensure that all projects and initiatives that may impact the process control systems are identified early in their life cycle and include appropriate security measures in their design.

- Identify and engage all projects that have process control systems implications at an early stage in their life cycle;
- Have a single point of accountability;
- Undertake security reviews;
- Plan for security testing at key points of the project development life cycle (e.g. tender, commissioning, factory acceptance testing and commissioning).

Establish Ongoing Governance

The objective of this stage is to provide clear direction for the management of process control system security risk and ensure ongoing compliance and review of the policy and standards. An effective governance framework provides clear roles and responsibilities, an up-to date policy and standards for managing process control security risk factors, and assurance that this policy and standards are being followed.

Requirements for a Practical Digital Identity System

"...That question is not what will the computer be like in the future, but instead, what will we be like? What kind of people are we becoming?"
Sherry Turkle, The second self, computers and the human spirit

Susan Morrow

Director of Research and Development at Avoco Secure Ltd
Susan.morrow@avocosecure.com
www.avocosecure.com

Humans now live in a dual world: On the one hand we live in what we term the 'real' world where we interact with other humans, most often face to face, or at least voice to voice, and on the other hand we live in a virtual world where we still need to interact with other human beings, but we do so in a much more covert and cryptic manner.

As we reside more and more in these dual universes we increase our need to replicate our real world experiences in our virtual domain. Just as we socialise in the real world, so we have created mechanisms that allow us to 'socialise' online. Just as we talk to each other in our real world, we have developed ways of communicating our thoughts and needs in our virtual world. This duality has led to a crisis in identity as an individual's identity and the trust implicit in that identity is the pivot upon which secure and true communications depend.

To begin our quest into what is or can become our digital identity, we need to begin with an understanding of the idea of 'who am I'.

The idea of a unique identity is a very philosophical idea, but one that is vital to our relationships with each other as well as our own personal placement in the world. Identification between individuals and groups is the foundation of our society and social intercourse. Subtle elements provide the requisite 'access control' required to tick the internal boxes that dictate the comfortable level of communication allowed with another individual. Without these clues to identity, none of us would have a framework on which to base our level of openness and expression: These social rules form the basis of our own self generated security restrictions. To augment our social identity and give it legal credence, our governments have built sets of paper-ware that define us through standardised procedures, for example passports.

The new world of PC personas requires the same sorts of interactions and communication. We need to take our *real world me* and export it to our *virtual world me* to make our virtual realm work. To begin our quest into what is or can become our digital identity, we need to begin with an understanding of the idea of 'who am I'. This starting point will allow us to determine the differences (if any) between our real and virtual world personas. Without understanding the reason for, and the evolution of, a person's identity, can we hope to define and develop identities that are usable within a virtual realm?

The questions of "what comprises our real world identity" and how we can frame this within a virtual platform needs to be answered before a system of digital identity can be created. There is little point in trying to dictate what an

identity is in terms of technology, when that decision is solely based on technical restraints; however a technical system for identity based on philosophy alone is also impractical. The best solution would be an informed technology based on the knowledge we have of the rules of social identity.

Dynamic Identities

How an individual's person is determined is a highly complex process not least complicated by the fact that the elements of identity can have dynamic qualities, changing throughout a person's lifetime. These dynamic parts, for example a name change after marriage, can have an impact on the use of that identity for different situations. The virtual world is an ideal platform for linking changing conditions to identity: For example, a persons digital identifier could be linked to a system that can associate information collated through some activity they take part in (perhaps financial transactions or an eBay feedback profile) to increase or decrease the trust level determined by such transactions – this can be equated to a trust factor weighting your identity. Weighted identities could then be used to confer or remove privileges.

...elements of identity can have dynamic qualities, changing throughout a persons lifetime

Group Identity, National Identity and European Identity

Kin selection and reciprocal altruism are defining social evolutionary methods of identifying like groups. These systems have evolved as a means of classifying groups of individuals so that survival behaviour can be optimised. For example, we are more likely to give food or money to a family member than a stranger. Similarly, we will give food or money to an individual that we have experience of being altruistic in return for favours.

Identifying kin or altruistic partners is a method of sharing identity within a system of classification. It is a way of defining a group of like individuals, whilst retaining their individual identity; if you like their individual identity becomes a sub-set of a larger identity grouping. It is an important analogy for the use of classes and identity within a digital world.

Just as our 'real world' identity builds upon our personal identity by including us in certain groups and excluding us from others, so in the digital realm should our identity be able to handle the inclusion of our individuality into a group based system whilst retaining the individuality of our identity for specific situations.

The idea of personal identity used within a digital arena to control a given process (e.g. access to a website) can be extended to include additional layers of identity that confer group membership. This type of classification system is already widely in use in applications such as Active Directory, etc. In this manner a person can have several sub-sets of identity, each having a different impact on how they can access or manipulate resources. In this way, the idea of a common European identity framework can exist in cohesion with national identities; this is true in particular in the virtual realm as having multiple levels of identity can translate into digital policies. The main issue is how to use the various layers of identity within a technological context, how to associate those identities and recognise them. If these layers can be associated through a common technology framework then linking a parameter based on membership of a national or European group onto an already existing personal identity, could be used to establish new sets of policies applicable to that person, within their multiple identity layer framing, creating a type multi-factor authentication system.

Using Identity to Control Digital Resources

The idea of weighting identity through transactional knowledge, or having multi-factor grouping of identity, is a way of determining the trustworthiness of an individual. Trust and identity are intrinsically connected and can be used to determine if a person can have access to resources or not. Adding additional parameters to a user's digital identity can potentially reap benefits in terms of controlling access to digital resources such a websites or information.

Problems with Current methods of Digital Identity

We already have in place a number of systems that can be used to identify a person within a virtual realm. Biometrics, digital certificates, shared secrets, *etc*. are abundant in their approach. This lack of standards is one of the problems associated with digital identity. Because there are so many systems available and because many of these systems need to be used by individuals, rather than managed by corporations, the choice and understanding of the underlying technologies can be very overwhelming for the average pc user. Digital certificates have an inherent problem with the understanding the idea of a 'key pair' and the distribution to others of the public part of the pair. Even in an organisation which can utilise IT resources to install and use digital certificates, the management of those certificates is often onerous. Similarly biometrics has inherent problems in real-time use. Biometrics seems like an obvious solution to creating digital identity, but a biometric system needs to be created and maintained, often involving costly hardware.

The applications to support this technology need to be developed so that biometrics can be used in a wider sphere, including information access control and online systems.
In addition, these systems are inherently restrictive in their application: they are not built upon the rules of social adaptation in the evolution of identity and as such will fall short of the flexibility needed in our ever-expanding virtual networks. However, this is not to say the underlying technology cannot be used as a platform to build upon, for example, linking a personal digital certificate with a group certificate issued on a nationality basis, could create a simple two-factor authentication methodology.

...the idea of a common European identity framework can exist in cohesion with national identities

Privacy Issues and Identity

We are continuously creating digital identities (on social networking sites, wiki's eBay, *etc*.) a process that is disjointed, untrustworthy, and not sustainable in the long term. If a system can be developed which truly applies an identity to a digital persona in a persistent and standard manner, then all of these varying concoctions of identity will become defunct, replaced by a reliable and truly identifiable digital persona.

Because by its very nature, a digital version of yourself is essentially decoupled from you; the information making up the virtual you is more difficult to control and so it can be used in a non-authorised manner both by criminals and potentially governments. Ensuring that an individual's personal information that comprises their identity is protected from misuse means that the method used to generate that identity in the first place must itself be secured. The use of multiple layers of identity based on individual parameters and group membership offers a potential mechanism for protecting the core identity itself; thus only coupled identities can be used for high value transactions, for example.

Summary

To achieve a usable and flexible system of digital identity that is workable in terms of allowing (or disallowing) access to resources we need to consider several things; the rules of social evolution of identity so that our digital persona is a real extension of ourselves, security of that digital persona so that we feel comfortable using it online, associating levels of identity based on group membership and most importantly a technology framework that can utilise the multiple levels of identity to generate policies for resource control. As a community we can work towards a unified identity system, but we must call upon the knowledge of many areas of expertise including evolutionary anthropology, philosophy and technology design.

1st International Conference on Critical Infrastructure Protection and Resilience (ICCR 2008)

The Swiss Federal Office for Civil Protection organises a first International Conference on Critical Infrastructure Protection and Resilience (ICCR) in the framework of the International Disaster and Risk Conference (IDRC). The event takes place from on August 26 and 27 in Davos, Switzerland, and addresses CIP issues relevant to decision-makers and practitioners from the public and private sector as well as researchers.

Stefan Brem

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

Blending resilience in CIP

Between 2003 and 2007, Switzerland - in partnership with Germany and NATO - has organised five international CIP events in the framework of the Euro-Atlantic Partnership Council (EAPC) and Partnership for Peace (PfP) Programme.
These EAPC/PfP workshops on Critical Infrastructure Protection (CIP) and Civil Emergency Planning (CEP) have attracted over the years more than 500 people, starting in 2003 with 60 people from 25 countries to 150 people from more than 40 countries in 2007.

Over the last four years the workshops have become a platform for inter-agency and public-private dialogue. It has started from rather general CIP and has addressed more concrete issues trying to integrate different sector specific perspectives in order to get a more comprehensive view.

Based on a mandate by the Federal Council (i.e. the Swiss Government) the Federal Office for Civil Protection has established a CIP working group including the relevant federal agencies. This working group has presented its first report to the Federal Council last July. Within the co-ordination task leading to a national CIP strategy the report has also stressed the importance of knowledge generation and information exchange as well as the role of facilitation of co-operation both nationally and internationally – with the public and private sector as well as academia.

It is therefore in this context that the Federal Office for Civil Protection organises a first International Conference on Critical Infrastructure Protection and Resilience (ICCR) in the framework of the International Disaster and Risk Conference (IDRC).

The ICCR particularly addresses the role of an integrated risk management in a CIP context and looks at public-private partnership concepts and applications. It also particularly addresses the role of resilience – both from a technical and a societal point of view. It also discusses possible criteria to define the criticality of infrastructures. In addition, the conference presents lessons learned responses to infrastructure failures.

Additional sessions on CIP will be held during the whole IDRC.

Further information on the ICCR can be found on the following website (associated conferences):
http://www.idrc.info/

ECN-9: Selected Links and Events

Actual Upcoming CIIP Conferences in Europe

- IST events, http://europa.eu.int/information_society/newsroom/cf/newsbytheme.cfm?displayType=calendar&tpa_id=7
- IT Sicherheit in der Produktionstechnik, June 16/17, 2008 in Stuttgart (in German): **www.it-produktionssicherheit.de/**
- 5th International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment DIMVA of GI SIG SIDAR, July 10-11, 2008 – Paris, France www.dimva2008.org
- 1st International Conference on Critical Infrastructure Protection and Resilience (ICCR 2008), August 26 and 27, 2008 in Davos, Switzerland: www.idrc.info
- 4th International Conference on IT-Incident Management & IT-Forensics www.imf-conference.org
- 3rd International Workshop on Critical Information Infrastructures Security, Call for Paper critis08.dia.uniroma3.it
- INFSO D4 events, http://cordis.europa.eu/ist/trust-security/events.htm
- Maritime Infrastructure Conference (link to the past conference Bahrain, Feb. 26-28, 2008, discussed in this issue: http://www.cusnc.navy.mil/articles/2008/013.html
- (Periodic conference, referenced in article) Global Government Critical Infrastructure Protection, Meridian 2007 conference in Stockholm http://www.meridianprocess.org/
- Security Analysis and Risk Management Association provides continuously events: http://SARMA.org/events/calendar/
- USA CIP Program's News and Events webpage (George Mason), http://cipp.gmu.edu/news/

European Projects or Projects with Articles in this Issue

- European Finance Forum: www.europeanfinanceforum.org
- DIESIS – Designing an Interoperable European federated Simulation network for Critical InfraStructures: www.diesis-project.eu
- DESEREC – DEpendability and Security by Enhanced REConfigurability: http://www.deserec.eu
- IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems: www.irriis.eu
- Federal Office for Information Security (BSI), www.bsi.de/english/index.htm
- German IT-Security handbook for basic protection: http://www.bsi.bund.de/gshb/intl/ index.htm

Standardisation on SCDA

- E-SCSIE: A working group of European actors for exchanging security information on SCADA and control systems: http://scni.jrc.it/03-projects/06-E-SCSIE/index
- ISA SP99, ISCI (ISA Security Compliance Institute) http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
- Process Control Systems Forum (PCSF) https://www.pcsforum.org

E-Reports

- The risk monograph can be accessed at http://cipp.gmu.edu/research/CIP_Risk_Monograph.php. Additional projects related to risk are underway, including the publication of a paper on regional (multi-jurisdictional) risk assessment and co-hosting of a conference on security analysis and risk management in May 2008.
- http://cipp.gmu.edu/ contains further information on the CIP Program and its work with respect to the numerous facets of critical infrastructure protection. The Program's website features a wealth of information on CIP; select research products and issues of its monthly newsletter, The CIP Report, are also available for download.
- www.cpni.gov.uk/ProtectingYourAssets/scada.aspx : effective Process Control Security framework which has been proven in practice and has been used to improve industrial control system security at a number of organisations, provided by the UK Government's Centre for Protection of National Infrastructure
- Reports to the article in the last ECN issue "SCADA Cyber Security, Critical Infrastructures' Achilles Heel?" can be requested on: http://www.s21sec.com/default.aspx?HIVEDATA=dW2z6ApW38XBhw8gB2U%2FUt58IVxnzmfIKSajF7JoZk%2Beu3%2Bw2Hl%2B4PAsozAswU%2FwfMmeRMWLI2ioGTTBH78h3%2FeU%2BDISajHmHdZVfBSu%2Fu4%3D

CRITIS'08

3nd International Workshop on Critical Information Infrastructures Security

October 13-15, 2008, Frascati (Rome), Italy

In the last years we observed dramatic changes in technological infrastructures that found the base of developed countries. For a lot of economical, social, technological and political reasons that are generally referred to as globalisation and liberalisation, they become more and more interoperable, integrated and interdependent. These phenomena and the actual socio-political instability, pose new and very hard challenges for 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 ICT that therefore has become a key-resource. At the same time ICT is considered as one of the most vulnerable elements of the whole system.
CRITIS'08 wants to bring together experts from science, industry and public authorities involved in management, supervision and protection of critical infrastructures to provide an interdisciplinary and multi-faceted view about third millennium security strategies for Critical Information Infrastructures.
Authors are solicited to contribute to the workshop by submitting articles that illustrate research results, R&D projects, surveying works and industrial experiences that describe significant advances in the following (non-exclusive) areas of Critical Information Infrastructures

- Modelling and Simulation of Critical Infrastructures
- Interdependency Modeling and Analysis
- Network and Organizational Vulnerability Analysis
- Threats and Attack Modeling
- SCADA/DCS and Control System Security
- Self-healing, Self-protection, Self-management Architectures
- Situation Awareness and Response Optimisation
- CIIP Policy and Cross-Border Issue
- R&D Agenda, Benchmarking and Survey

Instructions for paper submission
All submissions will be subjected to a thorough **blind review** by at least three reviewers. Papers should be up to 12 pages in English, including bibliography and well-marked appendices. As in the case of CRITIS'07, post-proceedings are planned to be published by Springer in the Lecture Notes in Computer Science series. Pre-proceedings will appear at the time of the conference. At least one author of each accepted paper is required to register with the workshop and present the paper.
To submit a paper, select the *Paper Submission* option in the menu and note the following. The submitted paper (in PDF or PostScript format), which should follow the template indicated by Springer, must start with a title, a short abstract, and a list of keywords. However, it should be anonymous with no author names, affiliations, acknowledgements, nor obvious references.
Revised and/or extended versions of outstanding papers from the conference will be published, on the base of their arguments, in a special issue of the *International Journal of Critical Infrastructure Protection (Elsevier)* or in a special issue of the *International Journal of System of Systems Engineering (Inderscience).*

Important dates

Submission of papers: May 15th, 2008
Notification to authors: July 15th, 2008
Camera-ready copies: August 31th, 2008

http://critis08.dia.uniroma3.it

IMF 2008
4th International Conference on
IT-Incident Management & IT-Forensics

September 23 - 25, 2008
Mannheim, Germany

www.imf-conference.org/
mailto:2008@imf-conference.org

Conference of **SIG SIDAR**
of the **German Informatics Society (GI)**.

Call for Papers: see www.imf-conference.org

Information technology has become crucial to almost every part of society. IT infrastructures have become critical in the world-wide economy, the financial sector the health sector, the government's administration, the military, and the educational sector. Although security usually gets involved into the design process of IT systems nowadays, the process of maintaining security in the operation of IT infrastructures, in most cases, still lacks the appropriate attention. The capability to manage and respond to IT security incidents and their forensic analysis are not well established. The quickly rising number of security incidents worldwide makes the implementation of incident management capabilities essential.

The scope of IMF 2008 is broad and includes, but is not limited to the following areas:

IT-Incident Management

- Purposes of IT-Incident Management
- Trends, Processes and Methods of IT-Incident Management
- Formats and Standardization for IT-Incident Management
- Tools for the IT-Incident Management
- Education and Training, IT-Incident Management Awareness
- Determination, Detection and Evaluation of Incidents
- Procedures for Handling Incidents
- Problems and Challenges when establishing CERTs/ CSIRTs
- Sources of Information/ Information Exchange/ Communities
- Dealing with Vulnerabilities (Vulnerability Response)
- Current Threats
- Early Warning Systems
- Organizations (National CERT-Associations, FIRST, TF-CSIRT, TERENA / TI, etc.)

IT-Forensics

- Trends and Challenges in IT-Forensics
- Methods, Processes and Applications for IT-Forensics .(e.g. Networks, Operating Systems, Storage Media, ICT Systems)
- Evidence Protection in IT-Environments
- Standardization of Evidence Protection Processes
- Data Protection and other legal implications for IT-Forensics
- Methods in Investigation
- Legal Relevance of IT-Forensics Investigations
- Tools for IT-Forensics
- IT-Forensics Readiness
-

IMPORTANT DATES

June 1, 2008:	Deadline for Submissions
June 23, 2008:	Notification of acceptance or rejection
July 14, 2008:	Final paper camera ready copy due
September 23-25, 2008:	IMF 2008 Conference

Call for Participation
Fifth Conference on Detection of Intrusions and Malware & Vulnerability Assessment

July 10-11th, 2008, Paris, France

Conference of SIG SIDAR of the German Informatics Society (GI)

The annual DIMVA conference serves as a premier forum for advancing the state of the art in intrusion detection, malware detection, and vulnerability assessment. Each year DIMVA brings together international experts from academia, industry and government to present and discuss novel research in these areas. DIMVA is organized by the special interest group Security - Intrusion Detection and Response of the German Informatics Society (GI). The conference proceedings will appear in Springer's Lecture Notes in Computer Science (LNCS) series.

Registration is now open at http://dimva2008.org/
Register before June 10th for early-bird discount

Keynote speakers

Richard Bejtlich Director of Incident Response, General Electric	**Tal Garfinkel** VMware/Stanford University

Preliminary program

- *A Tool for Offline and Live Testing of Evasion Resilience in Network Intrusion Detection Systems*
  Leo Juan, Christian Kreibich, Chih-Hung Lin and Vern Paxson
- *Data Space Randomization*
  Sandeep Bhatkar and R Sekar
- *Dynamic Binary Instrumentation-based Framework for Malware (Virus) Defense*
  Najwa Aaraj, Anand Raghunathan and Niraj K. Jha
- *Embedded Malware Detection using Markov n-grams*
  M. Zubair Shafiq, Syed Ali Khayam and Muddassar Farooq
- *Expanding Malware Defense by Securing Software Installations*
  Weiqing Sun, R. Sekar, Zhenkai Liang and V.N. Venkatakrishnan
- *FluXOR: detecting and monitoring fast-flux service networks*
  Emanuele Passerini, Roberto Paleari, Lorenzo Martignoni and Danilo Bruschi
- *Learning and Classification of Malware Behavior*
  Konrad Rieck, Thorsten Holz, Carsten Willems, Patrick Düssel and Pavel Laskov
- *On Race Vulnerabilities in Web Applications*
  Roberto Paleari, Davide Marrone, Danilo Bruschi and Mattia Monga
- *On the Limits of Information Flow Techniques for Malware Analysis and Containment* — Lorenzo Cavallaro, Prateek Saxena and R Sekar
- *The Contact Surface: A Technique for Exploring Internet Scale Emergent Behaviors*
  Carrie Gates and John McHugh
- *The Quest for Multi-headed Worms*
  Van-Hau Pham, Marc Dacier, Guillaume Urvoy-Keller and Taoufik En-Najjary
- *Traffic Aggregation for Malware Detection*
  Michael Reiter and Ting-Fang Yen
- *VeriKey: A Dynamic Certificate Verification System for Public Key Exchanges*
  Brett Stone-Gross, David Sigal, Rob Cohn, John Morse, Kevin Almeroth and Christopher Kruegel
- *XSS-GUARD: Precise Dynamic Prevention of Cross-Site Scripting Attacks*
  Prithvi Bisht and V.N. Venkatakrishnan

Organising Committee

General Chair: Hervé Debar, France Telecom R&D, France (info@dimva.org)
Program Chair: Diego Zamboni, IBM Zurich Research Lab, Switzerland (pc-chair@dimva.org)
Sponsor Chair: Ludovic Mé, Supélec (sponsor-chair@dimva.org)
Publicity Chair: Tadeusz Pietraszek, Google, Switzerland (publicity-chair@dimva.org)