Information & Security: An International Journal

Boyarchuk, Illiashenko, Kharchenko, Vain, vol.35, no. 1, 2016, 29-48

https://doi.org/10.11610/isij.3502

SEREIN PROJECT: MODERNIZATION OF POSTGRADUATE STUDIES ON SECURITY AND RESILIENCE FOR HUMAN AND INDUSTRY RELATED DOMAINS

Artem BOYARCHUK, Oleg ILLIASHENKO, Vyacheslav KHARCHENKO, and Jüri VAIN

Abstract: The paper presents the on-going EC-funded Tempus project TEMPUS SEREIN (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains, http://serein.net.ua) executed by consortia of academia and industry partners from Ukraine and EU countries. The state-of-the-art, completed work as well as the next steps of the development of teaching courses of master and doctoral level and in-service training modules on security and resilience for human and industry related domains are described.

Keywords: Security, resilience, master studies, PhD studies, European project, dissemination.

1 Introduction

Cyber terrorism is considered by EU&US governments to be the biggest threat currently facing the world.[1] As the world moves rapidly towards e-government, infrastructure, commerce and social activity we have introduced more effective, easier and low cost paths through which societies can be attacked. These paths are being exploited by organized crime as recent press reports have illustrated. Importance of securing business- and safety-critical systems may be proven by statistics:

- *E-commerce fraud*. In one year, e-fraud on domestic transactions went up 97 % to € 26.4 million in France [2];
- *Money laundering*.[3] In addition to the many traditional methods (including electronic funds transfer, fictional companies with foreign banks), other modern procedures, such as virtual casinos, have emerged on the Internet, growing up to 70 % in 2008 on comparison to 2006 (report of PwC 2009);

- There are a number of situations when complex use software and hardware vulnerabilities and faults have resulted in serious problems, e.g. Stuxnet – computer worm discovered in June 2010 − targets Siemens industrial software and equipment on five Iranian NPPs.[4,5]

It could be said that there are several challenges for current situation on cyber security in Ukraine:

- *Challenge 1 – Academic*: Certain isolation of a university science
- *Challenge 2 – Research*: Integration of safety and security requirements
- *Challenge 3 – Business*: Lack of high-class professional courses
- *Challenge 4 – Social*: Low support to motivated graduates to stay and make research in Ukraine.

As a result, there is a strong requirement for professional, sustainable and comprehensive staff provision in the domain of secure (critical) computer engineering, and the training of specialists in cyber security, exploiting the experience of leading universities using modern IT technologies. These gaps led to the development of the EC-funded Tempus project "Modernization of postgraduate studies on *SE*curity and *RE*silience for human and *IN*dustry related domains," or SEREIN.

The aim of this paper is to outline the contents of the SEREIN project and has the following structure: section 2 presents the objectives, project description and project structure, arisen problems and curriculum overview, section 3 contains information on National security alliance, section 4 gives a description of the consortium partners from Ukraine and EU, and section 5 contains synergy and interconnection of SEREIN with other projects funded under Tempus programme, conclusions and acknowledgements.

2 Project Description, Objectives and Structure

Background

The name of project is SEREIN, which is acronym from official name "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains". The project is financed by the TEMPUS programme, which encourages higher education institutions in the EU Member States and partner countries to engage in structured cooperation through the establishment of "consortia". Project duration: December 1, 2013 – November 30, 2016 (36 months).

TEMPUS SEREIN project (project reference number – 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCP), http://serein.net.ua/,[6] addresses the business and society demand on high qualified specialists on cyber security assessment and management by

introducing international master/doctoral/in-service programs on cyber security and resilience.

Existing Problems

A number of problems in Ukraine and EU member states adversely affect the quality of educational provision. Firstly, the absence of system harmonization of MSc and PhD programmes with EU standards for critical computing engineering and the Bologna Declaration. Secondly, the insufficient level of support for professional mobility of academic staff and graduates. More generally, there was the problem of an inadequate level of practical training of students due to the absence of well-equipped hi-tech resource laboratories.[7]

It is worth mentioning that some problems are common not only for technical universities of Ukraine but also for the other countries. Ukrainian government does not provide for the training of IT-specialists in a proper way and paying insufficient attention to specific aspects of studying cyber security and critical computing systems as a whole.

These above-mentioned troubles led to using MSc and PhD study programmes prepared without sufficient conformance to EC standards for cyber security. Furthermore, current courses of the MSc programmes did not correspond to constantly evolving complex information and communications technology systems – this situation led to the gap in education of young specialists compared with "bad guys". As a result of this some countries became extremely vulnerable in the e-world, as victims of politically motivated attacks e.g. Estonia, Ukraine, China, Georgia, Russian Federation, etc.[8,9] Such situation could lead to extremely bad consequences affecting the critical infrastructures which, in turn, will influence people by creating hazards and even losses. As an example of security and safety issues in critical infrastructure the instrumentation and control systems of nuclear power plants are reviewed by V. Kharchenko and his co-authors.[10]

Hardware security issues, hardware security and trust have become major concerns for national security over the past decade, and the development of tamper-resistant hardware devices made security functions become more and more complex task due to modern high-level techniques and tools needed for its breaking. This serves as an invaluable reference to the state-of-the-art research that is of critical significance to the security of, and trust in, modern society's microelectronic-supported infrastructures.[11-13]

Overview

The situation described above has stimulated the development of the SEREIN project idea and required a systemic approach to the development of project's objectives. As

a result, a team of experts was established which included the officials of Ukrainian and European universities, scientific centres, and companies experienced in training specialists and undertaking joint research in this domain. The expert team analysed the set of problems and developed the principles used in the development of the project proposal.

The key goal of the project is to produce new generation of engineering and research staff capable of performing constructive development in cyber security assessment and ensuring. This objective will contribute to fulfil the demand of Ukrainian society to face the challenges in the area of ensuring cyber security policy in different application domains.

Application domains are to be covered by developed master and doctoral in-service curricula as follows:

- Human (people, homeland);
- Business (banking; web & e-business; telecommunication);
- Safety Critical (aviation; space; NPP; power grid; railway).

Objectives of the Project

The SEREIN team aimed to achieve the following objectives:

- To develop master programme on cyber security and resilience with five courses;
- To develop doctoral programme on cyber security and resilience with three courses;
- To develop in-service training programme on cyber security and resilience with three modules;
- To establish a National Security Alliance (NSA) for training and consultancy in the area of cyber security assessment and management;
- To introduce a comprehensive capacity building scheme for involved academic staff of 7 Ukrainian universities.

To reach these objectives the international master and doctoral programmes on cyber security and resilience for Ukrainian universities will be developed.

Target Curriculum

According to the project proposal the following target courses need to be developed on the appropriate level of studies:

1. Master level:
    a. CM-1. Foundations of resilient computing
    b. CM-2. Systems and networks security and resilience

   c. CM-3. Human-machine engineering for resilient systems
   d. CM-4. Risk analysis of SoS [i] security and resilience
   e. CM-5. Secure and resilient PLD-based systems
2. Doctoral level:
   a. CP-1. Formal and "smart" methods for system security and resilience
   b. CP-2. Security and resilience of web- and cloud-systems
   c. CP-3. Security management systems
3. Systems In-service training level:
   a. CT-1. Techniques and tools for networks security assessment
   b. CT-2. Techniques and tools for industry FPGA-based systems security
   c. CT-3. Security and resilience assurance cases.

Target groups: students, trainees, teaching and administrative staff, top management of educational organizations, lecturers and researchers at the IT departments, engineering companies, local community administration staff.

The curriculum development will be based on the following steps:

1. Detailed needs assessment and planning of curricula and their placement for each university;
2. Knowledge transfer form EU (sharing and adapting curricula from EU partners, discussions, peer reviews, quality control, support to develop lecture books, guest lectures, support to development of processes), where all EU partners are involved;
3. Piloting of the curriculum will include Testing of Master/Doctoral curricula at all UA universities, placement of curricula with knowledge inputs from EU partners through guest lectures from City University and TUT.

The courses have to be defined in terms of the following structure: each of the courses consists of 3-4 modules, which reflects different theoretical and practical aspects on cyber security assessment, ensuring and management for described application areas. All modules have ECTS-compatible structure. The programme involves a number of practical case studies, thus, the special attention will be paid to the supporting literature for them. After successful finalization of the project the courses must be introduced at the target departments of the Ukrainian partner universities. These learn-

[i] SoS – Systems of Systems (critical infrastructures similar to smart power grids, etc.).

ing and pedagogical materials will establish the intellectual property framework for the National Security Alliance.

3 National Security Alliance

The aim of National Security Alliance (NSA) is to integrate all available and produced curricula, methods and tools for providing training and consultancy services in the area of cyber security assessment and management for institutions and industry acting in different application domains, such as:

- Human (people, homeland);
- Business (banking; web & e-business; telecommunications);
- Safety Critical (aviation; space; NPP; power grid; railway).

The structure of NSA comprises 7 offices to be incorporated at the involved department of each Ukrainian university from consortia: National Aerospace University KhAI (KhAI), University of Banking of the National Bank of Ukraine (USNBU), Khmelnitsky National University (KhNU), Dnipropetrovsk National University of Railway Transport (DIIT), Technology Institute of East Ukrainian National University (TI EUNU), Ternopil National Technical University (TNTU), Institute of Communications (ICSIS). Each office is specialized on the specific application domain with planned hardware/software and literature and thus is intended to be responsible for networking and cooperating of research and development, academic and industrial partners acting in the respective domain.

Department of computer systems and networks of National Aerospace University KhAI, is appointed as the leading office according to the preliminary partners' agreement. Each centre will include 2 rooms with the total floor space 60 sq. m. One room is intended for seminars/consulting sessions and the other room will accommodate the local NSA office director, expert and an assistant.

The consultants for the consulting/training subject areas are to be selected from the appropriate target departmental R&D staff and/or partner enterprise and employed via staff contract and paid through the income generated by respective NSA office. The functions of each office include training and consulting activities for wide target groups (MSc and PhD students, administrative R&D staff at partner universities and market customers) in the area of cyber security assessment and management:

1. Training of master and doctoral students based on the developed master programme on Security and Resilience (specific target group 1);
2. Providing in-service training sessions using the 3 developed in-service modules CT-A…CT-C. The lecturers from partner universities will be invited to

carry out the training event for a specific group of external participants in such seminar (specific target group 2);

a. CT-A. Modern Technologies of Security Assessment;

b. CT- B. Modern Technologies of Security and Resilience;

c. CT-C. Security Assurance Cases;

3. Providing consulting activities for the companies and individuals in the area of cyber security assessment and management (specific target group 3):

a. Creating & assessing risk methodologies;

b. End user security awareness training;

c. Penetration testing;

d. Security infrastructure architecture;

e. Security posture & risk assessments;

f. Vulnerability testing;

g. End user security awareness training;

h. Security infrastructure architecture.

The target groups of NSA (general target group of master and doctoral students at the target department of 7 Ukrainian universities):

- **UABNBU**: Department of Information Technologies and Systems (approx. 30 persons during 2015-2016 academic year);
- **TNTU**: Department of Computer Systems and Networks (approx. 60 persons during 2015-2016 academic year);
- **KhAI**: Department of Computer Systems and Networks (approx.. 85 persons during 2015-2016 academic year) and Department of Software Engineering (approx. 55 persons during 2015-2016 academic year);
- **ICSIS**: Department of Computer and Information Technologies and Systems (approx. 60 persons during 2015-2016 academic year) and Department of System Engineering (approx. 60 persons during 2015-2016 academic year);
- **DIIT**: Department of software systems (approx. 40 persons during 2015-2016 academic year) and Intelligent Transport Systems (approx. 35 during 2015-2016 academic year);
- **KhNU**: Department of Cybernetics and Computing Machinery (approx. 60 persons during 2015-2016 academic year);

- **TI EUNU**: Department of Computer Engineering (approx. 40 persons during 2015-2016 academic year).

Specific target groups of NSA:

1. Master and doctoral students of engineering specialties at different Ukrainian universities with developed master programme – no less than 700 persons;
2. External participants, individual and corporate customers, NGOs, local authorities applying for in-service training sessions – approx. 120 persons a year;
3. Regional and national R&D companies, individuals applying for consulting activities in the area of Cyber security assessment and management – approx. 70 customers a year.

4 Consortium Partners

SEREIN project proposal was submitted by the consortium of partners from Bulgaria, Estonia, Italy Sweden, UK, and Ukraine. Ukrainian partners have joined the consortium to cover all Ukrainian regions and all major applications of cyber security. SEREIN project was prepared in a form of agreement with the partners (i.e. organizations), which were responsible for particular tasks:

- Universities from Ukraine – development of teaching courses, training modules (long-life learning modules);
- Academia (research institutions) and industry partners from Ukraine – internal review consulting and support of dissemination of the developed courses;
- University, academia and industry partners from EU – internal review and consulting of the courses developed.

The selection of the partners for this project was achieved according to their experience in the domain of curriculum development in information security.

Ukrainian Partners

With 11,000 students and 2,700 academic staff, *National Aerospace University n. a. N.E. Zhukovsky "Kharkiv Aviation Institute,"* KhAI, http://www.khai.edu , is one of the leading institutions of higher education in Ukraine for the training specialists for the aircraft and aerospace industry in Ukraine and beyond. KhAI has branches in Mexico, Germany, Finland and China and it cooperates with first rate national and foreign manufacturers of aircraft engineering: "ANTONOV," "BOEING," "AIRBUS" and participates in the international programmes "ALPHA" and "SEA-LAUNCH." In addition, KhAI is one of the largest technical universities of Eastern

Ukraine. The Department of Computer Systems and Networks (CSN) carries out intensive research and methodical activities aimed at increasing the quality of engineering studies. The focus of research activities is on the development of methods, techniques, instrumental systems and tools for assessment, modelling, designing and expertise of dependable software, computer systems and networks for aerospace, atomic energy, medical and business-critical applications.

Institute of Communication, ICSIS, http://iszzi.kpi.ua, was established on December 27, 2006. Scientific capacity: 12 Doctors of Technical Sciences, 40 PhDs (similar to candidates of technical sciences) currently work in ISCIS today. One employee of ISCIS has been awarded a honorary degree "Honoured Science and Technology associate, and two others – "Honoured education employee of Ukraine." ISCIS has up-to-date material and technical base to organize qualitative educational process and scientific activity. The educational process is integrated into educational process of the university. Teaching of the part of humanities, social, economic, mathematic and natural-scientific disciplines is provided by academic staff of the university.

Founded in 1964, *Khmelnitskiy National University*, KhNU, http://www.khnu.km.ua, is one of the leading universities of Podolia – biggest historical region in southwestern part of Ukraine. With academic staff about 800 and student body 11.500 University includes 8 faculties and study graduates for 42 specialties. There are 15 scientific schools, 20 PhD specialties and 4 specialties for doctor of science degree studies. The Department of Systems Programming was established in 2004 from the staff of few other departments. The basic directions of the department's activities are as follows: intellectual decision making systems; diagnostics and fault-tolerance of microprocessor devices and complex systems. During last four years, the department has hosted the international conference "Computer Systems for Automation of Industrial Processes." The department actively participated in numerous research projects with EU and Polish national funding schemes.

Technological Institute of Volodymyr Dahl East Ukrainian National University (Severodonetsk), TI EUNU, http://www.sti.lg.ua. In TI EUNU the partner of TEMPUS SEREIN consortia is the Department of computer engineering which provides education for specialists in system integrated, computer-aided design and effective use of computerized and computer systems and networks in various fields of science, industry and business. Department of computer engineering carries out intensive research & methodical activities aimed at increasing the quality of engineering studies. The focus of research activities is on the development of methods, techniques & tools for industrial safety & ecology: risk investigation, human behaviour modelling, safety evaluation of human-machine systems, resilient and pervasive infrastructure, etc. The department has long-term and efficient cooperation with the largest Ukrainian chemical and refinery companies and regional municipalities.

The origins of the *Ternopil Ivan Pul'uj National Technical University*, TNTU, http://www.tntu.edu.ua, date back to 1960, when Ternopil All-technical Department of the Lviv Polytechnic Institute was organized. In 2007 P. Yasniy, Sc.D was appointed rector of TNTU. In 2009 the University granted the status of the National one. The general enrolment of students is around 5000 people. The amount of specialties for bachelors, specialists and masters reaches the number of 22 grouped into 19 directions. The training centres at the university are: Information technologies centre comprising the regional CISCO academy, regional centre for the certification of training specialists on the programs of Microsoft IT Academy & SUN Microsystems, the laboratory of the Shneider-Electric enterprise & certification, examination centre of the European Virtual University. The scope of research activities at the Department of Computer Systems & Networks includes the development of information systems for biometric authentication of person by dynamically typed signature; modelling & development of cryptanalysis algorithms using parallel & distributed computer systems.

Dnipropetrovsk National University of Railway Transport n. a. V. Lazaryan, DIIT, http://www.diit.edu.ua, is one of the largest higher educational institutions of railway transport in Ukraine. It was founded in 1930. Nowadays the structure of the university comprises 10 faculties, the number of students is more than 11000: 17 railway specialties and 8 – humanitarian-economic specialties. There are more than 700 scientific and pedagogical employees. The first engineers in the field of computer technologies and programming graduated from DIIT in 1964. There is Laboratory of information technologies with system of servers for development of Internet network of distance learning on which basis the system "Prometheus" of automated distant testing of students is implemented at university. The network is integrated with the branch network of railway for the distance learning of students.

The University of Banking of the National Bank of Ukraine (Kyiv), Ukraine, UABNBU, http://ubs.edu.ua/ua/. The University of banking of the National Bank of Ukraine (Kyiv) is a higher educational establishment of the 4-th level of accreditation. It was founded by the decision of the Cabinet of Ministers of Ukraine from June 15, 2006. University of Banking provides research, teaching and training activities and implements corporate social responsibility concept in its activity. The University of Banking is a unique, specialized institution which offers high-quality economic education and prepares specialists for the National Bank of Ukraine, commercial banks and other financial establishments. The University of Banking of the National Bank of Ukraine (Kyiv), including Lviv, Kharkiv and Cherkasy Institutes of banking, cooperates with 37 foreign educational establishments, banking institutions and consulting firms in different countries.

Research and Production Company "Radiy" (RADIY), http://www.radiy.com/en/, Kirovograd, Ukraine was founded in 1954. It was the largest manufacturer of television studio equipment, mobile TV stations, and broadcast transmitters in the former USSR. Now RADIY is the leading designer and manufacturer of safety critical digital instrumentation and control systems for NPPs with reactors of VVER-440 and VVER-1000. In addition, RADIY produces computer based fire-fighting systems, systems for power industry, etc. State Committee of nuclear regulations of Ukraine, State Company "EnergoAtom", State research centre of nuclear safety of Ukraine, Institute of nuclear research of National Academy of Sciences are among the partner institutions of RADIY.

The professional trade association *Ukrainian Security Industry Federation*, USIF, http://www.ufib.com.ua, was founded in 2007 and brings together manufacturers, distributors, integrators and installer's technical means of protection, automation and control systems engineering. Federation's mission is to promote a business environment of technical security, automation and control systems engineering new development strategy that is aimed at increasing the competitiveness of member companies and industries federation as a whole in the domestic and foreign markets. USIF is involved in the development of EU-harmonized standards and regulations for the Ukrainian market of security and automation systems & services. The membership of the Federation consists of more than 60 members who are the distributors, security agencies, system integrators, and centers of technical surveillance.

Ukrainian Students Association, USA, http://www.yss.com.ua. The idea of an independent professional association of students occurred in the summer of 1989. During December 8-9, 1989, the founding congress was held, which approved the Program Declaration and Charter of USA. USA's important task today is establishing self-government in schools and consolidating students' liberties in the Ukrainian legislation, the university statutes and documents of the Ministry of Education and Science of Ukraine. USA's structure consists of a primary union organization (cells). Primary organizations may have the status of district, city, borough and township branches of the Association. Primary organizations are united in the regional (oblast) branches of the USA. The membership body includes about 6,000 members. The structure of the governing bodies of association is as follows: Congress, the Coordination Council, and Board Chairman.

The company "Lime Systems," http://lime-systems.com, was created in November 1993. Today it is a team of highly qualified professionals with great experience in implementation of modern computer technologies in the banking system of Ukraine. In parts of development, implementation and maintenance works of about 90 highly qualified specialists, two of them are PhD. Project Management Institute (PMI) has assigned the management of company the status of Project Management Professional

(PMP). The company specializes in design, installation and maintenance of complex systems, banking automation, analysis of financial systems and specialized automation solutions. The company is the leading developer of banking software in Ukraine. The clients of the company are banking institutions such as ERSTE Bank Universalbank, FUIB Ukrgasbank, Kreditprombank, Rodovid Bank, Industrialbank, Megabank and many others. The development is based on Microsoft.NET technology, using the three-tier architecture.

Ministry of Education and Science of Ukraine, http://www.mon.gov.ua/, is the central body of the government executive power performing the management in the area of education. The key role of Ministry of Education and Science of Ukraine lies in the establishment of the education and state-level standards development program; leading the state policy in the area of education, science and professional training of specialists; ensuring the connection with educational institutions and government authorities of other countries with respect to issues of its competence; conducting accreditation of higher and vocational education institutes, issuing licenses and certificates to them.

The European Partners (Experts)

Tallinn University of Technology, TUT, Estonia, http://www.ttu.ee/, was founded in 1918, and has become one of the largest universities in Estonia. Being the flagship of Estonian engineering and technical education TUT has approximately 14,000 students and 2000 employees (incl. 1200 faculty members) as well as qualified professors with international experiences. The University is structured into eight faculties, three colleges and six research and development institutions. The Department of Computer Science is one of the youngest and most intensively evolving academic units at TUT. It was founded in December 2000. The department is a host institution for the bachelor and master level study programmes on Applied Computer Science, Software Engineering and Cyber Security (incl. Digital Forensics as sub-speciality). The research and development activities are carried out in the field of formal methods, semantics, software engineering, security, programming theory and others. Department has relations with many professional societies, universities and international organizations such as IEEE, IEE, IFAC, IFIP and others.

Royal Institute of Technology, KTH, Sweden, http://www.kth.se/en, is the largest technical university in Sweden. KTH is actively participating in major EU cooperation programmes such as FP7, Lifelong Learning, Tempus, Erasmus-Mundus, Asia-Link and Leonardo da Vinci. Several national and international competence centres and networks of excellence are located at KTH. Its research programmes cover broad range of cyber security areas from basic research projects to applied research in close co-operation with internationally leading universities and industries. The domain of

activities includes systems, enterprise architecture modelling and analyses with respect to information and cyber security, secure networked control etc.). KTH is the leader in different local and international projects in cyber security: VIKING (cyber security for critical infrastructure), Security system for mobile agents etc. Cyber security programs integrate different institutions and groups focused on cyber security: KTH School of Electrical Engineering (Industrial Information and Control Systems, Laboratory for Communication Networks), School of Information and Communication Technology (Laboratory for Computer Security and Security Informatics), ACCESS Linnaeus Centre etc.

City University London, UK, http://www.city.ac.uk/. The Centre for Cyber and Security Sciences at City University was created in early 2011 by drawing together focused groups concentrating on network security, computer security, software reliability, information security etc. City University endorses the published UK and EU strategies on cyber security and has organized its resources to support the strategies and to focus on the threats posed. The Centre will be able to apply the techniques of systems science and systems analysis to the complex issues posed by illicit cyber activity in order to identity effective solutions as we believe in outcome related research. Also, the Centre for Software Reliability (CSR) as an independent research centre in the School of Informatics at City University was founded in 1983. CSR is one of the world's major players in dependability research, especially in the areas of quantitative assessment and of diversity from 1980s.

Institute of Information and Communication Technologies, IICT, Bulgaria, http://www.iict.bas.bg/EN/. The Institute of Information and Communication Technologies, Bulgarian Academy of Sciences (IICT-BAS) is the leading Bulgarian state research body in the multi-aspect field of ICT Developments for Emerging Security Challenges. The staff of IICT-BAS consists of 265 people and the research staff includes 148 people and 40 PhD students working in 15 departments. The “IT for Security Department” has been organized in IICT-BAS. The department encompasses a Centre for Security and Defence Management (targeting mainly security & defence policies and analysis) and a Joint Training, Simulation, and Analysis Centre (targeting applied operational analysis and computer assisted exercises). Its team explores, advances and applies methodologies and tools for modelling and simulation for the security sector, including information/cyber security management.

Consorzio Interuniversitario Nazionale per l’Informatica, CINI, Italy, http://www.consorzio-cini.it/, is a non-profit consortium of 35 public Italian Universities for research in computer science and engineering. The consortium is under surveillance of the Ministry for Education, University and Research. CINI participates to the project through the research unit of the Department of Computer and Systems Engineering (DIS, www.dis.unina.it) of the Federico II University of Naples that hosts

the CINI National Laboratory "C. Savy". The Federico II University is the second largest university in Italy. DIS is typically involved in EU projects in informatics through the CINI Laboratory "C. Savy", founded in 2000. The Laboratory participated in the following EU projects: the IST Program projects CADENUS, INTERMON, NETQoS, OneLab, and OneLab2; the Networks of Excellence E-NEXT and CONTENT; the FP7 projects INTERSECTION and INSPIRE; the Marie Curie IAPP project Critical-Step and the Support Action Osmosis. DIS is currently involved in the TEMPUS project SAFEGUARD with Ukrainian partners.

Together the project partners establish a team which has all the necessary resources for implementation of the project and the production of all planned outcomes. The function of the internal verification (experts from Ukraine) of each course has been assigned to the representatives of the organizations responsible for the development of the corresponding courses. European experts have been assigned to the developers' teams according to their excellence (see Table 1).

5. Synergy and Interconnection of SEREIN with Other Projects

SEREIN developed programmes are logical continuation of the MSc and PhD programmes on critical software and computing developed in the frame of MASTAC [14] and National Safety IT-engineering network of centres established by innovative academia-industry handshaking framework SAFEGUARD.[15]

SEREIN project is even more closely connected with two more undergoing projects funded by Tempus programme – CABRIOLET and GREENCO.

GREENCO project "Green Computing and Communication" (2012-2015), grant holder Newcastle University.[16, 17] The aim of the project is the development of master and doctoral degree programmes on green computing and communications. Among the special tasks lays the establishment of two PhD incubators on Green IT engineering. Through this master programme the close cooperation links between national research and development institutions and university systems will be spanned and high quality of education in a higher education system in green computing and communications programs will be enhanced. Target MSc and PhD programmes are intended for IT bachelor graduates to gain an understanding of the green computing methodologies and paradigms, energy efficient system level software such as compilers, hypervisors, monitoring and profiling tools, workload managers, and programming environments, energy aware large scale distributed systems, such as Grids and Clouds. It is suitable for those aspiring to be software developers, software architecture designers, FPGA developers, experts on distributed infrastructures.

Table 1: SEREIN project responsibilities matrix.

Courses	*Developers teams*	*UA experts*	*EU experts*
CM1. Foundations of resilient computing	TNTU, KhAI	RPC Radiy	KTH, Sweden
CM2. Systems and networks security and resilience	DIIT, UABNBU, ICSIS, TNTU	USIF	CityU, UK
CM3. Human-machine engineering for resilient systems	KhAI, TNTU, TI EUNU	RPC Radiy	KTH, Sweden
CM4. Risk analysis of SoS security and resilience	TI EUNU, KhAI	USIF	CityU, UK
CM5. Secure and resilient PLD-based systems	KhAI, TNTU, DIIT	RPC Radiy	TUT, Estonia
CP1. Formal and intellectual methods for system security and resilience	KhNU, KhAI	RPC Radiy	CINI, Italy
CP2. Security and resilience of web-, cloud- systems	KhAI, KhNU	USIF	KTH, Sweden
CP3. Security management systems	ICSIS, DIIT	USIF	IICT, Bulgaria
CT1. Techniques and tools for networks security assessment	UABNBU, TNTU, ICSIS	USIF	CINI, Italy
CT2. Techniques and tools for industry FPGA-based systems security	KhAI, TNTU, DIIT	RPC Radiy	TUT, Estonia
CT3.Security and resilience assurance cases	KhAI, KhNU, UABNBU	RPC Radiy	IICT, Bulgaria

CABRIOLET project "Model-oriented approach and intelligent knowledge-based system for evolvable academia-industry cooperation in electronic and computer engineering" (2013-2016), grant holder Newcastle University.[18-19] The project is aimed

on the design and nation-wide sustainable introduction of model-oriented approaches based on implementation of general life cycle model of Evolvable Academia-to-Business Cooperation (EA2BC). Also, 3 customized models serving different types of Academia-to-Business cooperation have been proposed. Among the other outcomes, the project implemented an intelligent knowledge-based system (IKBS) for analysis, processing and generating of assessment results and recommendations for involved academic departments and companies.[20] In order to establish such sustainable system the results of GreenCo project are qualitatively and effectively used. The overall picture of synergy of SEREIN project with other projects is described in detail in a report by V. Kharchenko and team.[21] Figure 1 shows briefly cross-fertilizing interrelations.

The project management team has identified also the main risk factor to be taken into consideration during the project lifecycle. Possible changes in the Ministry and State Accreditation Committee politics could have a negative impact on the project implementation. To avoid these problems all project activities will be performed with the involvement of a number of specialists from the Ministry and Committee to ensure continuous support of the performed activities.

6 Conclusions

Modern information and communication technologies actively became more complex and hence new challenges and their interconnections arise particularly for computing: problems of security (vulnerabilities and threats assessment), safety (hazards, common cause failure prediction), green (green metrics, and energy consumption and modes of operation) and dependability, etc. It is important to address these groups of challenges to institutions of higher education in order to prepare qualified specialists who will be able to defend (and attack if needed) instrumentation and control systems and critical infrastructures based on leading edge information and communication technologies. This activity needs adequate training and educational activities on all level of studies starting from background at bachelor level, going through master and doctoral programmes towards to lifelong learning and in-service trainings for professional development. In order to organize education of such specialists SEREIN consortium is trying to build the educational space for representation of different challenges on cyber security in critical computing.

To date the development of the master/doctoral/in-service programs on cyber security and resilience in the frame of SEREIN is under development, the harmonization process of results is undergoing within the consortium organizations.

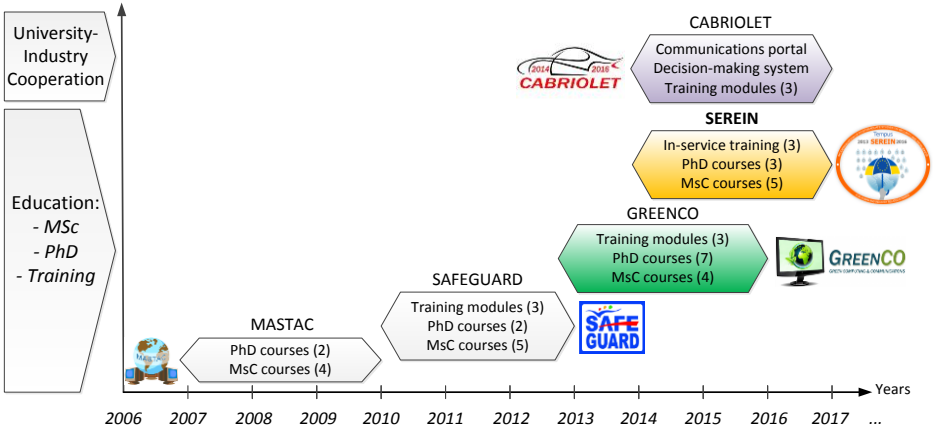

Figure 1: Synergy and interrelation of SEREIN and other Tempus projects.

Finally, through dissemination activities the project will make the results public and validate the findings of its developments, its relevance and usefulness. The pilot deployment of results is made throughout the higher technical educational system within Ukraine (with application to cyber security) through an International conference of practitioners, academics and EU experts, and through articles in the academic and research press.

The project team is convinced that the obtained results and developed courses will be useful not only for Ukrainian universities but also for other EU countries' acting in the field of training specialists in the area of cyber security and critical IT-technologies.

Acknowledgments

The coordinators express their thanks to the EU members from different organizations for their interest in the project and for their continued assistance in the various activities. We thank to all British (Dr. P. Popov, Prof. R. Bloomfield, et. al.), Estonian (Dr. M. Krispin, et. al.), Italian (Prof. S. Russo, Prof. D. Cotroneo, Prof. M. Cinque, et. al.), Bulgarian (Prof. T. Tagarev), Swedish (Dr. V. Kordas) colleagues providing all-round scientific and methodical support of development and discussion of SEREIN courses.

We are, of course, indebted to the course development teams, in particular the course leaders (Prof. A. Gorbenko, Prof. I. Skarha-Bandurova, Prof. A. Ryazantsev, Prof. O. Potii, Prof. O. Pomorova, Prof. V. Mokhor, Dr. I. Brezhniev, Dr. A. Gordieiev) and

experts from “Radiy” (Dr. A. Siora, Prof. V. Sklyar, Dr. O. Odarushchenko), USIF (Mr. A. Biriukov) since without them it would not be possible to realize the intended outcomes, as well as master and doctoral students who have been involved in curriculum development.

References

1. Christopher Harress, “Obama says cyberterrorism is country's biggest threat, U.S. Government Assembles ‘Cyber Warriors’,” *International Business Times*, 18 February 2014, http://www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337.
2. François Paget, *Financial Fraud and Internet Banking: Threats and Countermeasures*, McAfee report (Santa Clara, CA: McAfee, 2009), http://cfile24.uf.tistory.com/attach/132B5C184B6B6D8155F8F4.
3. Brett Wolf, HSBC loses senior anti-money laundering compliance executive, *Reuters*, 11 October 2015, www.reuters.com/article/2015/10/11/hsbc-compliance-idUSL1N1292CO20151011.
4. The Stuxnet Worm, Norton by Symantec, http://us.norton.com/stuxnet.
5. Ralph Langner, “Stuxnet’s Secret Twin,” *Foreign Policy*, 19 November 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.
6. TEMPUS SEREIN project website http://serein.net.ua/.
7. Vyacheslav Kharchenko, Chris Phillips, Peter Popov, Oksana Pomorova, Alexander Romanovsky, and Elena Troubitsyna, “MASTAC: New Curriculum for Master and Doctoral Studies in Critical Software and Computing,” in *Proceedings of the 2008 International workshop on Software Engineering in East and South Europe SEESE’08*, Leipzig, Germany, 13 May 2008, pp. 59-64, https://doi.org/10.1145/1370868.1370879.
8. Jose Nazario, “Politically Motivated Denial of Service Attacks,” NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf.
9. Jason Richards, “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security,” *International Affairs Review*, http://www.iargwu.org/node/65.
10. Michael Yastrebenetsky, Vyacheslav Kharchenko, et al., *Nuclear Power Plant Instrumentation and Control Systems for Safety and Security* (Hershey, PA: IGI Global, 2014). − 470 pp., https://doi.org/10.4018/978-1-4666-5133-3.

11. Ted Huffmire, Cynthia Irvine, Thuy D. Nguyen, Timothy Levin, Ryan Kastner, and Timothy Sherwood, *Handbook of FPGA Design Security* (Dordrecht: Springer, 2010). – 177 pp., https://doi.org/10.1007/978-90-481-9157-4.

12. Benoit Badrignans, Jean-Luc Danger, Viktor Fischer, Guy Gogniat, and Lionel Torres, eds., *Security Trends for FPGAs: From Secured to Secure Reconfigurable Systems* (Springer, 2011). – 196 pp., https://doi.org/10.1007/978-94-007-1338-3.

13. Mohammad Tehranipoor and Cliff Wang, eds., *Introduction to Hardware Security and Trust* (New York, NY: Springer, 2012), https://doi.org/10.1007/978-1-4419-8080-9.

14. Kharchenko, et al., "MASTAC: New curriculum for master and doctoral studies in critical software and computing."

15. Vyacheslav Kharchenko, Chris Phillips, and Artem Boyarchuk, "TEMPUS-SAFEGUARD: National Safety IT-engineering Network of Centres of Innovative Academia-Industry Handshaking," *Information & Security: An International Journal* 28, no. 2 (2012): 315-318, https://doi.org/10.11610/isij.2825.

16. TEMPUS GreenCo project website: http://my-greenco.eu.

17. Vyacheslav Kharchenko, Oleg Illiashenko, Chris Phillips, and Jüri Vain, "Green Computing within the Context of Educational and Research Projects," in *Recent Advances in Computer Science, Proceedings of the 19th International Conference on Computers* (part of CSCC'15), Zakynthos Island, Greece, 16-20 July 2015, pp. 513-518, http://www.inase.org/library/2015/zakynthos/COMPUTERS.pdf.

18. TEMPUS CABRIOLET project website: http://www.my-cabriolet.eu.

19. Vyacheslav Kharchenko, Yuriy P. Kondratenko, "Analysis of Peculiarities of Innovative Collaboration between Academic Institutions and IT Companies in Areas S2B and B2S," *Technical News* 39-40 (2014): 15-19, − in Ukrainian, http://technicalnews.net.ua/library/2014/15.pdf.

20. Yuriy P. Kondratenko, "Revolution in Computer Science and Engineering and Its Impact on Evolution of Higher Education," in Revolución, Evolución e Involución en el Futuro de los Sistemas Sociales (Barcelona: Real Academia de Ciencias Económicas y Financieras, 2014), pp 129-159, https://racef.es/archivos/publicaciones/09_yuri_m37.pdf.

21. Vyacheslav Kharchenko, Oleg Illiashenko, Artem Boyarchuk, Chris Phillips, Juri Vain, and Madli Krispin, "FPGA-based Critical Computing: TEMPUS and FP7 Projects Issues," in *Proceedings of the 10th European Workshop on Microelectronics Education*, EWME, Tallinn, Estonia, 14-16 May 2014, 74-79, https://doi.org/10.1109/EWME.2014.6877399.

About the Authors

Artem BOYARCHUK, Oleg ILLIASHENKO, and Vyacheslav KHARCHENKO are with the National Aerospace University KhAI, Kharkiv, Ukraine. Jüri VAIN is Professor at the Department of Computer Science, Tallinn University of Technology, and coordinator of the SEREIN project.