ICS Security Related Working Groups, Standards and Initiatives

For the Report : Good practices for an EU ICS testing coordination capability

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu**.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-074-1 doi: 10.2824/26451

Table of Contents

1 Introduction

This document provides an overview of existing working groups, standards and pilots in the area of Industrial Control System Testing. The results of this document have been revised and filtered to include the last changes as well as to extract the relevant documents with respect to the ICS Testing sector. The way in which the information is organised has been adapted to the objectives of this study. To this regard, is worth noting that all descriptions being provided for each of the documents are directly extracted from the document itself or from the website of the organization(s) behind them.

It takes into account activities of international and national organizations, important activities in Europe and the US, as well as the most important branch specific activities (international and national). The first table group indicates diferents working groups which the main objetive are the ICS testbed activities. The results of this document have been revised and updated to include the last changes as well as those identified new guidelines, standards and regulations in the next section of tables. The last part, initiatives refers all projects, initiatives, laboratories and pilots related with ICS Testbed sector.

What follows is an introduction to the different information fields that have been included into the tables.

Working Groups (European and International) fields:

- **Name**: Name of the Working Group.
- **Type**: Association, Private non-profit association, Private Organization, Public-Private partnership.
- **Mision/Objectives**: Objectives to the Working Group.
- **Activities related**: Activities performing by the working group related with testbed.
- **Results**: Date of publication of the draft/final version of the standard, guideline or regulatory document.
- **Comments**: Important information not included in other fields.
- **URL**: URL in which full information can be found.
- The values of the "Type" field can be one of the following:
  - **Industry association:** An association that supports and protects the rights of a particular industry and the people who work in that industry, and which seeks to achieve the common goals of its members. There may be a public entity within these associations, but it does not have a leading role.
  - **Public Private Partnership:** A government service or private business venture which is funded and operated through a partnership of government and one or more private sector companies.
  - **Public body:** An organization whose work is part of the process of government, but is not a government department.
  - **Private non-profit association**: organization that uses surplus revenues to achieve its goals rather than distributing them as profit or dividends.
  - **Professional association:** Also called a professional body, professional organization, or professional society. A professional association is usually a non-profit organization seeking to represent a particular profession, the interests of individuals engaged in that profession, and the public interest.

- **Industry partnership**: An industry partnership is a multi-employer collaborative effort that brings together management and labor around the common purpose.
- **Consortium**: Association of two or more individuals, companies, organizatitons or governments (or any combination of these entities) with the objectives of participating in a common activity or pooling their resources for achieving a common goal.

Standards fields:

- **Name:** Name of the standard
- **Type:** Guideline, recommendation, regulation, report, standard, technical report.
- **Group / initiative / organisation:** Group, initiative or organisation responsible for the creation of the standard, guideline, regulation, recommendation, report or technical report.
- **Status:** Draft, Final [revision x |version x], special edition.
- **Publication date:** Date of publication of the draft/final version/special edition of the standard.
- **Addressed Industry:** All, Generic (ICS in general), chemistry, electricity distribution/transportation, oil and gas distribution, etc.
- **Geographic relevance:** Country where the standard is valid.
- **Related standards:** Other identified standards, guidelines, or regulatory documents which have a strong relationship with the document being described.
- **Description:** Short description on the content of the standard.

Initiatives (European and International) fields:

- **Project name:** Name of the initiatives.
- **Organisation name:** Organisation name in which the initiatives has been performed.
- **Brief project description:** Short description on the content of the initiative.
- **Period:** Validity period to the initiative.
- **Country:** Country where the initiativehas been created.
- **Environment:** Generic, electricity, energy, water, etc
- **URL:** URL in which full information can be found.

2 Working Groups

2.1 International

Name	UCA International Users Group (UCAIUG)
Type	Industry association
Mision/Objectives	The UCA International Users Group is a not-for-profit corporation focused on assisting users and vendors in the deployment of standards for real-time applications for several industries with related requirements. The mission of the UCA International Users Group is to enable integration through the deployment of open standards by providing a forum in which the various stakeholders in the energy and utility industry can work cooperatively together as members of a common organization.
Activities related	• Influence, select, and/or endorse open and public standards appropriate to the energy and utility market based upon the needs of the membership. • Specify, develop and/or accredit product/system-testing programs that facilitate the field interoperability of products and systems based upon these standards. • Implement educational and promotional activities that increase awareness and deployment of these standards in the energy and utility industry. • Influence and promote the adoption of standards and technologies specific to the ever-increasing smart grid initiatives worldwide. Besides, UCA International Users Group assess control systems and communication protocols for vulnerabilities that could put critical infrastructures at risk from a cyber attack. Advanced Metering Infrastructure Security (AMI-SEC) Task Force under the UtiliSec Working Group helps UCA in this task.(1)
Results	Users guides, industry education, transfer of technology, marketing support, identification of users needs and industry demonstrations to prove concepts. IEC 61850-10 Conformance Testing
Comments	
URL	http://www.ucaiug.org

Name	Deparment of Energy (DOE)
Type	Public Platform
Mision/Objectives	The mission of the Energy Department is to ensure America's security and prosperity by addressing its energy, environmental and

	nuclear challenges through transformative science and technology solutions. Catalyze the timely, material, and efficient transformation of the nation's energy system and secure U.S. leadership in clean energy technologies. Maintain a vibrant U.S. effort in science and engineering as a cornerstone of our economic prosperity with clear leadership in strategic areas. Enhance nuclear security through defense, nonproliferation, and environmental efforts. Establish an operational and adaptable framework that combines the best wisdom of all Department stakeholders to maximize mission success.
Activities related	**DOE Transmission Reliability Program** The Transmission Reliability Program worked with 3M, Oak Ridge National Laboratory (ORNL), and the Tennessee Valley Authority (TVA) to develop, evaluate, and test advanced highcapacity conductors. In a cooperative effort, DOE, ORNL, 3M, and TVA designed and built a high-current test facility at ORNL to evaluate conductors, accessories, and sensors under accelerated conditions by cycling those to high load levels over an extended period of time. ORNL performed outdoor thermal testing on the ACCR conductor and its accessories to evaluate their overall sag and temperature performance compared to design specifications. Future possible testing activities on overhead conductors include: • Testing indoors in a unique facility with a 56-foot ceiling and 1,400-foot length, and; • Testing conductors at full-system voltage (161kV) and current. In addition, these facilities can be used for: • Configuring and testing power electronic systems for transmission system control; • Developing and testing sensors for transmission system monitoring, and; • Testing superconducting devices.
Results	**CALiPER program** This program supports testing of a wide array of SSL products available for general illumination. DOE allows its test results to be distributed in the public interest for non-commercial, educational purposes only. Detailed test reports are provided to users. DOE publishes CALiPER Summary Reports following completion of a testing series. Each Summary Report focuses on a single product type or application. Detailed Reports provide extensive data on individual products tested through the CALiPER program and are distributed in the public interest for non-commercial, educational purposes only. CALiPER Benchmark Reports, published periodically, provide detailed analysis of test results for both traditional (non-LED) and LED products for a given application, comparing a range of standard lighting measures. An finally, the DOE CALiPER Program conducts and

	publishes advanced exploratory studies on issues related to testing of lighting technology and applications.
Comments	U.S. Department of Energy
URL	http://energy.gov/

Name	ISA and ISA99 commitee
Type	Professional association
Mision/Objectives	ISA's mission is to become the standard for automation globally by certifying industry professionals; providing education and training; publishing books and technical articles; hosting conferences and exhibitions for automation professionals; and developing standards for industry. The purpose of the ISA99 committee is to develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance. The Committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for industrial automation and control and provide criteria for procuring and implementing secure control systems. Compliance with the Committee's guidance will improve system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing degradation or failure of the equipment or process under control.
Activities related	• Facilitate the independent testing and certification of control system products to a defined set of control system security standards; • Use existing control system security industry standards, where available, develop or facilitate development of interim standards where they do not already exist, and adopt new standards when they become available; • Accelerate the development of industry standards that can be used to certify that control systems products meet a common set of security requirements. • The standards, tests, and conformanc e processes for control systems products will allow the products to be securely integrated. The ultimate goal is to push the conformance testing into the product development life cycle so that the products are intrinsically secure.
Results	Standards, technical reports, certification programs, training, publications, conference and exhibits.
Comments	
URL	http://www.isa.org/

	http://isa99.isa.org/ISA99%20Wiki/Home.aspx

Name	National Institute for Standards and Technology (NIST)
Type	Public body
Mision/Objectives	NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST maintains ongoing contact with a broad spectrum of users through a variety of means, including but not limited to public meetings, public workshops, individual contacts, and formal and informal collaborations and partnerships, to ensure that the information it disseminates continues to remain relevant. NIST attends and holds public workshops, conferences, and meetings to gather input about what types of information would be useful to industry; universities; other not-for-profit entities; and Federal, state, and local governments; and maintains memberships in many industry groups for the purpose of facilitating such discussions.
Activities related	NIST's activities are: • Development of performance metrics, measurement and testing methods, predictive modeling and simulation tools, knowledge modeling, protocols, technical data, and reference materials and artifacts • Evaluation of technologies, systems, and practices, including uncertainty analysis. • Development of the technical basis for standards and practices—in many instances via testbeds, consortia, standards development organizations, and/or other partnerships with industry and academia. NIST's activities are organized into laboratory programs, and extramural programs. In October 2010, NIST was realigned by reducing the number of NIST laboratory units from ten to six. NIST Laboratories include: • Engineering Laboratory (EL) • Information Technology Laboratory (ITL) • Material Measurement Laboratory (MML) • Physical Measurement Laboratory (PML) • Center for Nanoscale Science and Technology (CNST) • NIST Center for Neutron Research (NCNR) NIST has created an Industrial Control Security Testbed inside NIST Programs of the Manufacturing Engineering Laboratory program. NIST has developed government-wide identification card standards for federal employees and contractors to prevent unauthorized persons from gaining access to government buildings and computer systems.

Results	NIST is one of the most important standardisation organizations in the USA. They have developed several standards on ICS security, It can be highlighted the following ones: • NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security. (2) • NIST SP 800-53, Recommended Security Controls for Federal Information Systems. (3) • Field Device Protection Profile for SCADA Systems in Medium Robustness Environments. (4) • NIST IR 7176, System Protection Profile – Industrial Control Systems. (5) NIST has also defined a security smart grid workgroup to develop an overall cyber security strategy for the Smart Grid. This overall strategy includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure. This group has created the following document of interest: • NISTIR 7628, Guidelines for Smart Grid Cyber Security. (6)
Comments	
URL	http://www.nist.gov

Name	NIST SGIP/CSWG
Type	Professional association
Mision/Objectives	The primary goal is to develop an overall cyber security strategy for the Smart Grid that includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure. The cyber security strategy needs to address prevention, detection, response, and recovery. Implementation of a cyber security strategy requires the definition and implementation of an overall cyber security risk assessment process for the Smart Grid. The following objectives address the CSWG's primary goal. These objectives may change as more Smart Grid implementations occur and Smart Grid technologies further develop. These objectives include: • Assessing Smart Grid Interoperability Panel (SGIP) identified standards within an overall risk assessment framework that focuses on cyber security within the Smart Grid. • Developing a set of recommended security requirements that may be used by strategists, designers, implementers, and operators of the Smart Grid, (e.g., utilities, equipment manufacturers, regulators) as input to their risk assessment process and other tasks in the security life cycle of a Smart - Grid information system. These security requirements are

	intended as a starting point for organizations. • Identifying Smart Grid specific problems and issues that currently do not have solutions. • Creating a logical reference model of the Smart Grid, which will enable further work towards the creation of a logical architecture and a security architecture. This work is being performed in coordination with the SGIP Architecture Committee (SGAC). • Identifying inherent privacy risk areas and feasible ways in which those risks may be mitigated while at the same time supporting and maintaining the value and benefits of the Smart Grid. • Developing a conformity assessment program for security requirements in coordination with activities of the SGIP Smart Grid Testing and Certification Committee (SGTCC).
Activities related	Members of the CSWG assist in defining the activities and tasks of the CSWG, attend the SGIP and SGIP Governing Board (SGIPGB) meetings, and participate in the development and review of the CSWG subgroups' projects and deliverables. SGIP-CSWG Standing Sub-groups: • AMI Security Subgroup • Architecture Subgroup • Design Principles Subgroup • High-Level Requirements Subgroup • Privacy Subgroup • Research and Development (R&D) Subgroup • Standards Subgroup • Testing and Certification Subgroup The CSWG have several working subgroups(AMI Security Subgroup, Architecture Subgroup, Design Principles Subgroup, High-Level Requirements Subgroup…) but the SGTCC develop a guidance and recommendations on Smart Grid conformance, interoperability, and cybersecurity testing. The guidance and processes developed will be for the utility sector laboratories and utilities conducting cybersecurity and/or interoperability testing to evaluate Smart Grid systems, subsystems, and components. The Testing and Certification (TCC) subgroup, created in 2010, establishes guidance and methodologies for cybersecurity testing of Smart Grid systems, subsystems, and components. The subgroup focuses on developing cybersecurity testing guidance and test cases for Smart Grid systems, subsystems, and components for their hardware, software, and processes, and assisting the SGIP SGTCC and internal NIST Smart Grid conformance projects.
Results	Technical reports (NIST IR 7628)
Comments	The Smart Grid Interoperability Panel–Cyber Security Working Group

	(SGIP-CSWG) was formerly known as the Cyber Security Coordination Task Group (CSCTG) Smart Grid Interoperability Panel Cyber Security Working Group
URL	http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Name	Smart Grid Testing&Certification Committee (SGTCC) WG
Type	Committee
Mision/Objectives	The SGTCC's mission is to coordinate creation of documentation and organizational frameworks relating to compliance testing and certification to Smart Grid interoperability and cybersecurity standards. The SGTCC's objectives include the development of an action plan, with the support of relevant parties, to establish a standardized framework (e.g., tools, materials, components, and examples) that can be used by those performing testing for and certification of compliance with interoperability and cybersecurity standards. (7)
Activities related	Since its establishment, SGTCC has undertaken a number of activities in the framework development process. The action plan of the SGTCC describes the plans and deliverables to be developed through the SGTCC. It is a living document that evolves through close collaboration with industry stakeholders to ensure that identified issues and needs in framework development and implementation are addressed by the SGTCC.
Results	SGTCC has developed a framework to enable industry testing and certification programs for Smart Grid interoperability.(8) Key SGTCC Documents: • IPRM Version 2 • ITCA Development Guide and FAQs • IPRM FAQs • Smart Grid Testing Landscape • Testing White Paper • Draft 2013 SGTCC Outreach Plan - for review / comment. • Interoperability Process Reference Manual, Version 1.0 • T&C Landscape Report • T&C Framework Development Guide • SGTCC 2011 Roadmap • SGTCC 2010 Roadmap
Comments	SGTCC members are a diverse and elected group including manufacturers, end users and test labs. The SGTCC contains many working groups focused on a variety of testing and certification issues (SGTCC Catalog of Standards Working

	Group, IPRM Implementation Work
URL	http://www.sgip.org/smart-grid-testing-certification-committee-sgtcc/

Name	Critical Infrastructure Security Working Group (CISSWG)
Type	Association
Mision/Objectives	DOE's Office of Energy Assurance established CISSWG, a standards group to serve as a clearinghouse for critical energy infrastructure security standards development. Their goals include coordinating and influencing international and industrial standards activities, providing technical leadership, and facilitating oversight in order to improve US energy security through the adoption of beneficial technologies and security practices.
Activities related	The NSTB Program funded the Critical Infrastructure Security Standards Working Group (CISSWG) to identify industry standards applicable to control system security and to perform an initial evaluation of the scope and status of those standards.
Results	Technical reports
Comments	
URL	Aditional information can be located in http://www.sandia.gov

Name	DETER Enabled Federated Testbeds (DEFT) consortium
Type	Consortium
Mision/Objectives	The DETER Enabled Federated Testbeds (DEFT) consortium is a collaborative effort to bring to a broader audience cyber-physical resources that are geographically distributed and the tools necessary to explore and analyze results in the cyber-physical space. The members of the DEFT consortium are the Pacific Northwest National Laboratory (PNNL), the Information Trust Institute at the University of Illinois at Urbana-Champaign, the Information Sciences Institute (ISI) at the University of Southern California, SRI International, and the U.S. Department of Homeland Security. Each member of the consortium brings strong capabilities and domain expertise that are necessary to realize a state-of-the-art integration of cyber-physical resources in an automated and repeatable fashion.(9)
Activities related	The DEFT consortium is building upon the past successes of the DETER project at ISI to realize control system integration with the robust cyber experimentation capabilities of the DETER framework. In doing so, DEFT strives to add many extensible capabilities, pushing the state of the art in both testbed development and cyber-physical experimentation.

Results	Collaborators in DETER project
Comments	
URL	http://deter-project.org/

Name	Information Trust Institute (ITI)
Type	Academic / Industry partnership
Mision/Objectives	ITI aims to create a new paradigm for designing trustworthy systems from the ground up and validating systems that are intended to be trustworthy. ITI's research is organized into five themes: • Data Science • Evaluation: Evaluation testbed development.(10) • Health Information • Power Grid • Systems & Networking
Activities related	ITI faculty and students are developing mathematical models, methodologies, and tools for modeling system behavior and assessing correctness, and are creating test-bed-based experimental methodologies for assessing trust.
Results	Test-bed-based experimental methodologies for assessing trust like: **Illinois Center for a Smarter Electric Grid (ICSEG)** (11) The Illinois Center for a Smarter Electric Grid (ICSEG) is a 5-year project that develops and operates a facility at the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign to provide services for the validation of information technology and control aspects of Smart Grid systems, including micro grids and distributed energy resources. The key objective is to test and validate within a laboratory setting how new and more cost-effective Smart Grid technologies, tools, techniques, and system configurations can be used in trustworthy configurations that significantly improve upon the ones that are in common practice today. The laboratory is becoming a resource for Smart Grid equipment suppliers and integrators and electric utilities to allow validation of system designs before deployment. **Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)** This work is funded by the Department of Energy, with support from the Department of Homeland Security. Researchers from the University of Illinois at Urbana-Champaign, Dartmouth College, Cornell University, the University of California at Davis, and Washington State University are together addressing the challenge of how to protect the nation's power grid by

	significantly improving the way the power grid infrastructure is built, making it more secure, reliable, and safe.
Comments	ITI's education programs recognize the crucial role of workforce development in ensuring the future of trustworthy information systems. Major ongoing education efforts include an annual summer intern program that attracts promising undergraduates from aro
URL	http://www.iti.illinois.edu

Name	ISA99 standards development committee
Type	Committee
Mision/Objectives	ISA 99 Committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for industrial automation and control and provide criteria for procuring and implementing secure control systems. Compliance with the Committee's guidance will improve system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing degradation or failure of the equipment or process under control.
Activities related	To develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance. Guidance is directed towards those responsible for designing, implementing, or managing industrial automation and control systems as defined in the committee scope. This guidance also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.
Results	Standards, recommended practices, technical reports, and related information
Comments	
URL	http://www.isa.org/

Name	ISA Security Compliance Institute (ISCI)
Type	Consortium
Mision/Objectives	• Establish a set of well-engineered specifications and processes for the testing and certification of critical control systems products. • Decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders.

Activities related	The ISA Security Compliance Institute, which supports effective implementation of industry standards via compliance testing, market awareness, technical support, and education.
Results	Specifications and processes for the testing and certification of critical control systems products like ISASecure EDSA.
Comments	
URL	http://www.isasecure.org

Name	AGA 12 Task Group
Type	Professional association
Mision/Objectives	The AGA 12 Task Group was mandated to offer initially a short-term retrofit solution for existing systems and later a long-term solution applicable to new systems and internet-based SCADA communicaations. The purpose of the AGA 12 Task Groups is to save time and effort on the part of SCADA system owners by offering them a comprehensive system designed specifically to protect SCADA communications. One of the things AGA 12 stresses is that the use of cryptographic protection is effective only if it is deployed as a component of a comprehensive set of cyber security policies combined with adequate attention to the physical security of the utility's infrastructure.
Activities related	AGA 12 Task Group decided to split the AGA-12 report into four parts and the first of them is: “AGA-12, Part 1: Cryptographic Protection of SCADA Communications: Background, Policies and Test Plan”. AGA 12 Task Group encourages other expert groups to perform complexity-theoretic analysis and publish their findings.
Results	Reports, practices and policies
Comments	
URL	www.aga.org

2.2 European

Name	Deutsches Institut für Normung (DIN)
Type	Private organization
Mision/Objectives	DIN's primary task is to work closely with involved stakeholders to develop consensus-based standards that meet market requirements. Some 26,000 experts contribute their skills and experience to the standardization process.By agreement with the German Federal Government, DIN is the acknowledged national standards body that

	represents German interests in European and international standards organizations. Ninety percent of the standards work now carried out by DIN is international in nature. Tasks and objectives of DIN: • Ensuring the participation of all stakeholders regardless of their economic position and language skills • Promoting the free movement of goods through active involvement in international and European standardization • Holding the secretariats of international committees • Adopting European and international standards at national level • Maintaining the uniformity and consistency of the standards collection • Actively contributing to consensus building • Taking legal regulations into consideration • Providing an electronic infrastructure for standards development • Avoiding duplication of work DIN represents Germany’s standardization interests as a member of the European Committee for Standardization (CEN). DIN holds almost 30% of all CEN working committee secretariats.
Activities related	DIN, the German Institute for Standardization, offers stakeholders a platform for the development of standards as a service to industry, the state and society as a whole. Din is one of the associated to develop VDI/VDE 2182.
Results	Standards and reports
Comments	Deutsches Institut für Normung or The German Engineering Society
URL	http://www.din.de

Name	EuroSCSIE
Type	Public Private Partnership
Mision/Objectives	It was formed in June 2005 confidentially to share mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions in the SCADA and Control Systems environment. EuroSCSIE aim: • Sharing mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions (testing results for example); • Acting as cross-country facilitator for the exchange of best practices and information;

	• Supporting the EU-Countries policy makers on the matter of Critical Infrastructure Protection EuroSCSIE topics: • Sharing of incidents and good practices • Questionnaire on Control Sustem Cyber-Security (aimed at vendors) • Standards and requirements • Self assessment tools • Smart grids
Activities related	This test bed uses realistic environments with the appropriate resources for conducting independent verification and validation tests. These tests include, at least: • Check the compliance of applications and systems with specific security profiles. • Verify and validate that programming good practices and methodologies are being applied. • Certify that ICT security tools and services are compatible with specific ICS systems, applications and specific setups.
Results	Information exchange, technical documents, guidelines
Comments	EURO-SCSIE is, at this moment, composed, among the others, by the following organizations: • The European Organization for Nuclear Research (CERN-Geneve) • The Global Cyber Security Center • The Dutch Ministry of Economic Affairs • The Dutch National Infrastructure Cyber Crime (NICC) • The German Federal Office for Information Security (BSI) • The Hungarian CERT • The Joint Research Centre of the European Commission (JRC) • The Norwegian NorCERT • The Danish GovCERT • The Swedish Emergency Management Agency (SEMA) • The European Network and Information Security Agency (ENISA) • The Finnish Civil Protection • The Swiss Federal Office of Police • The Swiss Federal Strategy Unit for IT (ISB) • SwissGrid (Switzerland) • EDF • The U.K. Centre for the Protection of National Infrastructure (CPNI).
URL	https://espace.cern.ch/EuroSCSIE/default.aspx

Name	EU-US Expert Subgroup
Type	Public-Private Partnership
Mision/Objectives	Information sharing, awareness raising, incident response and test bed coordination
Activities related	• Information sharing: Exploring the creation of an EU-US publicprivate trusted network covering the most relevant aspects of ICS and Smart Grids, including energy sector, governments, IT, telecom, vendors, integrators, academia and research institutions. • Awareness Raising: Fostering awareness raising on cyber security of ICS and Smart Grids through high quality events involving all types of stakeholders and with special attention to top management (CEOs) commitment. • Incident Response: Fostering cooperation at transnational level, based on national ICS Security Strategies, established national ICS-CERTs, in cooperation with an adequate number of public and private CERTs. • Test bed coordination - R&D: EU and US will mutually support each other in the development and maintenance of ICS and Smart Grid test beds and collaborate in knowledge exchanging.
Results	Guidelines, education and training and research and technology demonstration tools
Comments	
URL	

3 Guidelines, Standards and Regulations

Name	A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)
Type	Guideline
Group / initiative / organisation	Systems and Network Analysis Center, National Security Agency
Status	Version: 1.1
Publication date	August 2010
Addressed Industry	Generic
Geographic relevance	US
Related standards	FIPS Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security (2)

Description	This guideline offers a cost-benefit analysis approach which will allow to prioritize the defensive efforts by identifying network security improvements that provide the greatest benefit for a given cost. It has discussed a process of assessing the potential impact or loss incurred by successful compromise of networked ICS assets or network links. Once a prioritized list has been created, a cost effective risk management approach to addressing system vulnerabilities may occur. Conducting active testing on critical, in-service ICS network segments and equipment can cause potential consequences. Because of these dangers, it is always best to conduct active service scans of critical ICS devices by staging "cloned" devices on a test network. Embedded ICS devices can be "cloned" by using similar models with comparable settings/configuration. PCs can be "cloned" using hard drive duplication software like Norton/Symantec Ghost.

Name	Critical Infrastructure Protection: Challenge and Efforts to Secure Control System
Type	Recommendations
Group / initiative / organisation	GAO (United States General Accounting Office)
Status	Version: 1.0
Publication date	March 2004
Addressed Industry	Generic
Geographic relevance	US
Related standards	
Description	To reduce the vulnerabilities of the control system, officials from one company formed a team composed of IT staff, process control engineers, and manufacturing employees. This team worked collaboratively to research vulnerabilities and to test fixes and workarounds. Government, academia, and private industry have independently initiated multiple efforts and programs focused on some of the key areas that should be addressed to strengthen the cybersecurity of control systems. One report includes a detailed discussion of many initiatives. One of the key areas include the following effort: • **Research and development of new security technologies to protect control systems.** Both federal and nonfederal entities have initiated efforts to develop encryption methods for securing communications on control system networks and field devices. Moreover, DOE is planning to establish a National SCADA Test Bed to test control system

	vulnerabilities. However, funding constraints have delayed the implementation of the initial phases of these plans. • **Development of requirements and standards for control system security**. Several entities are working to develop standards that increase the security of control systems. The Process Controls Security Requirements Forum (PCSRF), established by NIST and NSA, is working to define a common set of information security requirements for control systems. In addition, the North American Electric Reliability Council (NERC) is preparing to draft a standard that will include security requirements for control systems. • **Increased awareness of security and sharing of information about the implementation of more secure architectures and existing security technologies**. To promote awareness of control system vulnerabilities, DOE has created security programs, trained teams to conduct security reviews, and developed cybersecurity courses. The Instrumentation Systems and Automation Society (ISA) has reported on the known state of the art of cybersecurity technologies as they are applied to the control systems environment, to clearly define what technologies can currently be deployed.

Name	ISO/IEC 17025
Type	Standard
Group / initiative / organisation	ISO/IEC
Status	Second edition
Publication date	2005
Addressed Industry	Generic
Geographic relevance	Worldwide
Related standards	ISO/IEC 17000, Conformity assessment — Vocabulary and general principles VIM, International vocabulary of basic and general terms in metrology ISO 5725-1, 2, 3, 4, 6 ISO 9000 ISO 9001:2000 ISO/IEC 90003 ISO 9001:2000 ISO 10012:2003

	ISO/IEC 17011 ISO/IEC 17020 ISO 19011 ISO Guide 30, 31, 32, 33, 34 and 35 ISO/IEC Guide 43-1, 2 ISO/IEC Guide 58:1993e ISO/IEC Guide 65
Description	ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories is a standard used by testing and calibration laboratories. This international standard specifies the general requirements for the competence to carry out tests and/or calibrations, including sampling. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods. This standard is applicable to all organizations performing tests and/or calibrations. This international standard is applicable to all laboratories regardless of the number of personnel or the extent of the scope of testing and/or calibration activities. When a laboratory does not undertake one or more of the activities covered by this international standard , such as sampling and the design/development of new methods, the requirements of those clauses do not apply. If testing and calibration laboratories comply with the requirements of this International Standard, they will operate a quality management system for their testing and calibration activities that also meets the principles of ISO 9001. In this standard managements requirements are proposed regarding Organization, Management system, Document control, Review of requests, tenders and contracts, Subcontracting of tests and calibration, Purchasing services and supplies, Service to the customer, Complaints, Control of nonconforming testing and/or calibration work, Improvement, Corrective action, Preventive action, Control of records, Internal audits, Management reviews. Regarding technical requiremententes there are many factors that determine the correctness and reliability of the tests and/or calibrations performed by a laboratory. These factors include contributions from: • Human factors • Accommodation and environmental conditions • Aest and calibration methods and method validation • Equipment • Measurement traceability • Sampling • The handling of test and calibration items

	After undertaking the tests assuring the quality of test and calibration results are neccesary. The resulting data shall be recorded in such a way that trends are detectable and, where practicable, statistical techniques shall be applied to the reviewing of the results. This monitoring shall be planned and reviewed and may include, but not be limited to, the following: • Regular use of certified reference materials and/or internal quality control using secondary reference materials; • Participation in interlaboratory comparison or proficiency-testing programmes; • Replicate tests or calibrations using the same or different methods; • Retesting or recalibration of retained items; • Correlation of results for different characteristics of an item. Finally, the results of each test, calibration, or series of tests or calibrations carried out by the laboratory shall be reported accurately, clearly, unambiguously and objectively, and in accordance with any specific instructions in the test or calibration methods.

Name	ISO/IEC 21827
Type	Standard
Group / initiative / organisation	ISO/IEC
Status	Second edition
Publication date	2002
Addressed Industry	Generic
Geographic relevance	Worldwide
Related standards	ISO/IEC 21827-2002 ISO/IEC 27000-2009 ISO/IEC 27001-2005 ISO/IEC 27004-2009 ISO/IEC 27035-2011 ISO/IEC 15946-1-2008 ISO 19790 CORR 1-2008 ISO/TR 140-830-2010 ISO/IEC 27007-2011 ISO/IEC TR 27015-2012

Description	ISO/IEC 21827:2008 specifies the Systems Security Engineering - Capability Maturity Model (SSE-CMM), which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. ISO/IEC 21827:2008 does not prescribe a particular process or sequence, but captures practices generally observed in industry. The model is a standard metric for security engineering practices covering the following: • the entire life cycle, including development, operation, maintenance and decommissioning activities; • the whole organization, including management, organizational and engineering activities; • concurrent interactions with other disciplines, such as system, software, hardware, human factors and test engineering; system management, operation and maintenance; • interactions with other organizations, including acquisition, system management, certification, accreditation and evaluation. The objective is to facilitate an increase of maturity of the security engineering processes within the organization. The SSE-CMM is related to other CMMs which focus on different engineering disciplines and topic areas and can be used in combination or conjunction with them.

Name	NERC CIP 002-009-4
Type	Standard
Group / initiative / organisation	North American Electric Reliability Corporation (NERC)
Status	Revision 4, revision 5 is under aprobation
Publication date	2011
Addressed Industry	Electricity transportation/distribution
Geographic relevance	North America
Related standards	
Description	NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

	Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets. Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment. Standard **CIP-002-4** requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. Standard **CIP-003-4** requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard **CIP-004-4** requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard **CIP-005-4a** requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard **CIP-006-4c** is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard **CIP-007-4** requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). The requirement R1 talks about 'Test Procedures' and it explains that the Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware. • The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation. • The Responsible Entity shall document that testing is performed in a manner that reflects the production environment. • The Responsible Entity shall document test results.

	Standard **CIP-008-4** ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. The requirement R1 says that the Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following: • Procedures to characterize and classify events as reportable Cyber Security Incidents. • Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans. • Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary. • Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes. • Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually. • Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Standard **CIP-009-4** ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices

Name	NIST 800-115
Type	Guideline (Technical report)
Group / initiative / organisation	National Institute of Standards and Technology (NIST)
Status	Final
Publication date	September 2008
Addressed Industry	Generic
Geographic relevance	Worldwide
Related standards	SP 800-30 SP 800-37 SP 800-40 SP 800-53

	SP 800-53A SP 800-64 SP 800-84 SP 800-88 SP 800-92 SP 800-94
Description	This document is a guide to the basic technical aspects of conducting information security assessments. It presents technical testing and examination methods and techniques that an organization might use as part of an assessment, and offers insights to assessors on their execution and the potential impact they may have on systems and networks. For an assessment to be successful and have a positive impact on the security posture of a system (and ultimately the entire organization), elements beyond the execution of testing and examination must support the technical process. Suggestions for these activities—including a robust planning process, root cause analysis, and tailored reporting—are also presented in this guide. The processes and technical guidance presented in this document enable organizations to: • Develop information security assessment policy, methodology, and individual roles and responsibilities related to the technical aspects of assessment • Accurately plan for a technical information security assessment by providing guidance on determining which systems to assess and the approach for assessment, addressing logistical considerations, developing an assessment plan, and ensuring legal and policy considerations are addressed • Safely and effectively execute a technical information security assessment using the presented methods and techniques, and respond to any incidents that may occur during the assessment • Appropriately handle technical data (collection, storage, transmission, and destruction) throughout the assessment process • Conduct analysis and reporting to translate technical findings into risk mitigation actions that will improve the organization’s security posture. To accomplish technical security assessments and ensure that technical security testing and examinations provide maximum value, NIST recommends that organizations: • **Establish an information security assessment policy**. This identifies the organization’s requirements for executing assessments, and provides accountability for the appropriate

	individuals to ensure assessments are conducted in accordance with these requirements. Topics that an assessment policy should address include the organizational requirements with which assessments must comply, roles and responsibilities, adherence to an established assessment methodology, assessment frequency, and documentation requirements. • **Implement a repeatable and documented assessment methodology**. This provides consistency and structure to assessments, expedites the transition of new assessment staff, and addresses resource constraints associated with assessments. Using such a methodology enables organizations to maximize the value of assessments while minimizing possible risks introduced by certain technical assessment techniques. These risks can range from not gathering sufficient information on the organization's security posture for fear of impacting system functionality to affecting the system or network availability by executing techniques without the proper safeguards in place. Processes that minimize risk caused by certain assessment techniques include using skilled assessors, developing comprehensive assessment plans, logging assessor activities, performing testing off-hours, and conducting tests on duplicates of production systems (e.g., development systems). Organizations need to determine the level of risk they are willing to accept for each assessment, and tailor their approaches accordingly. • **Determine the objectives of each security assessment, and tailor the approach accordingly**. Security assessments have specific objectives, acceptable levels of risk, and available resources. Because no individual technique provides a comprehensive picture of an organization's security when executed alone, organizations should use a combination of techniques. This also helps organizations to limit risk and resource usage. • **Analyze findings, and develop risk mitigation techniques to address weaknesses**. To ensure that security assessments provide their ultimate value, organizations should conduct root cause analysis upon completion of an assessment to enable the translation of findings into actionable mitigation techniques. These results may indicate that organizations should address not only technical weaknesses, but weaknesses in organizational processes and procedures as well.

Name	NIST 800-53
Type	Guideline (Technical report)

Group / initiative / organisation	National Institute of Standards and Technology (NIST)
Status	Revision 4
Publication date	April 2013
Addressed Industry	Generic
Geographic relevance	Worldwide
Related standards	NIST SP 800-39 NIST SP 800-137
Description	This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). The security and privacy controls are customizable and implemented as part of an organization - wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy.

Name	Process Control Domain (PCD) – Security Requirements for Vendors
Type	Regulation (Industrial Mandate)
Group / initiative / organisation	WIB, EI and EXERA (EWE)
Status	Final (revision 2)
Publication date	October 2010
Addressed Industry	Generic

Geographic relevance	France, UK, The Netherlands
Related standards	N/A
Description	This document specifies requirements and gives recommendations for IT security to be fulfilled by vendors of process control & automation systems to be used in Process Control Domains (PCDs). Four Process Areas (PA's) domains are used to separate the basic characteristics of the security engineering process from the management and institutionalization characteristics. PAs consist of all practices that define security engineering. These practices are called Base Practices (BPs) and are designated Bronze, Silver or Gold to indicate the level of security maturity defined by achieving the Base Practice and appointed Requirement Enhancements. There are 35 defined PAs that are organized into four logical categories: • **Organizational PAs** include BP requirements and Requirement Enhancements for policies and procedures. • **System Capability PAs** include BP requirements and Requirement Enhancements for security functions to be designed into the Vendor's system, and compensating security functions used to protect Vendor system components and subsystems which do not have built-in security capabilities. • **System Acceptance Testing and Commissioning PAs** include BP requirements and Requirement Enhancements for demonstrating correct implementation of security functions built into the Vendor's system, and readiness of system turnover for operation by the Principal or selected Operator. • **Maintenance and Support PAs** include BP requirements and Requirement Enhancements for demonstrating correct maintenance of security functions built into the Vendor's system, and timely support in response to security related events. Unit testing and Factory Acceptance Testing (FAT) are performed by the Vendor at the Vendor's site. Unit tests are usually performed in accordance with an Engineering test script and the results are documented in an Engineering report. Successful completion of unit tests is the basis for engineering to declare the Vendor's system ready for formal FAT. It is assumed that FAT is performed in accordance with predefined/approved procedures and acceptance criteria. Furthermore, FAT tests are witnessed by Quality Assurance representatives from the Vendor and Principal who sign-off and certify that the test is completed satisfactorily. Satisfactory completion of all FAT tests results in the readiness to ship the Vendor's system to the Principal for System Acceptance Testing and Commissioning. Readiness to ship is the milestone which completes FAT defines the "as-built" Vendor system.

	System Acceptance Testing (SAT) is performed by the Vendor at the end user's site. It is assumed that SAT is performed in accordance with predefined/approved procedures and acceptance criteria. Furthermore, SAT tests are witnessed by Quality Assurance representatives from the Vendor and End user who sign-off and certify that the test is completed satisfactorily. Satisfactory completion of all SAT tests results in commissioning the Vendor's system for operation and turn-over to the End user for operations. Turn-over is the milestone which completes SAT and Commissioning and begins the Maintenance and Support phase of the Vendor's system life cycle.

Name	ISA 99
Type	Standard
Group / initiative / organisation	ISA
Status	3rd edition
Publication date	2007
Addressed Industry	Generic
Geographic relevance	American National Standard
Related standards	ANSI/ISA-84.00.01 Part 1 and Part 3. ANSI/ISA-95.00.01 ANSI/ISA-95.00.03 ISO/IEC 7498. IEC 61508-4. ANSI/IEC 62443.
Description	The ISA99 series addresses electronic security within the industrial automation and control systems environment. The series will serve as the foundation for the IEC 62443 series of the same titles, as being developed by IEC TC65 WG10, "Security for industrial process measurement and control - Network and system security". Concepts, Terminology and Models. This standard establishes the context for all of the remaining standards in the series by defining the terminology, concepts and models to understand electronic security for the industrial automation and control systems environment. **ANSI/ISA-TR99.01.02-2007** (previously named ANSI/ISA-TR99.00.01-2007), Security Technologies for Manufacturing and Control Systems. This Technical Report (TR) describes various security technologies in

	terms of their applicability for use with industrial automation and control systems. This report will be updated periodically to reflect changes in technology. **ANSI/ISA-99.02.01-2009,** Establishing an Industrial Automation and Control Systems Security Program. This standard describes the elements to establish a cyber security management system and provides guidance on how to meet the requirements for each element. **ANSI/ISA-99.02.02** (in development), Operating an industrial automation and control system security program. This standard will address how to operate a security program after it is designed and implemented. This includes the definition and application of metrics to measure program effectiveness. **ANSI/ISA–99.03.xx** (in development), Technical security requirements for industrial automation and control systems (in development). These standards will define the characteristics of industrial automation and control systems that differentiate them from other information technology systems from a security point of view. Based on these characteristics, the standards will establish the security requirements that are unique to this class of systems. For further information refer to (ESCoRTS Project, 2009).

Name	IEC 61850 -Communication networks and systems for power utility automation. Part 10, Conformance testing.
Type	Standard
Group / initiative / organisation	IEC technical committee 57: Power systems management and associated information exchange
Status	Second Edition
Publication date	2011
Addressed Industry	Electrical
Geographic relevance	International
Related standards	IEC 61850-4 IEC 61850-6 IEC 61850- 7-2, 7-3 and 7-4 IEC 61850-8-1 and 9-2IEC 61850 ISO 9646
Description	Specifies standard techniques for testing of conformance of implementations, as well as specific measurement techniques to be

applied when declaring performance parameters. The use of these techniques will enhance the ability of the system integrator to integrate IEDs easily, operate IEDs correctly, and support the applications as intended. Defines a testing methodology in order to determine “conformance” with the numerous protocol definitions and constraints defined in the document.

The major technical changes with regard to the previous edition are as follows:

- Server device conformance test procedures have been updated
- Client system conformance test procedures have been added
- Sampled values device conformance test procedures have been added
- (Engineering) Tool related conformance test procedures have been added- GOOSE performance test procedures have been added

The tests defined in part 10 of the standard involve communication from a Device Under Test (DUT) to a test system. The following areas are covered:

- Inspection of the documentation and version control of the device (According to IEC 61850-4);
- Test of device configuration file against standardized syntax (According to IEC 61850-6);
- Test of device configuration file against the device related object model (IEC 61850-7-3 and 7-4);
- Test of communication stack implementation (IEC 61850-8-1 and 9-2);
- Test of implemented ACSI services against their definition (in IEC 61850-7-2);
- Test of device specific extensions according to rules given by the IEC 61850 series in general.

The test procedure requirements are:

- The abstract test cases describe what shall be tested, the detailed test procedures describe how a test engineer or a test system shall perform the test.
- Test cases include a reference to the applicable paragraph(s) in the referenced document(s).
- The test results shall be reproducible in the same test lab and in other test labs.
- Support automated testing with minimal human intervention, as far as reasonably possible.
- The tests shall focus on situations that can’t easily be tested during, for example, a factory or site acceptance test, and prevent inter-operability risks, for example:
  - check behaviour of the device on delayed, lost, double

	and out of order packets, • configuration, implementation, operation risks, • mismatching names, parameters, settings, or data types, • exceeding certain limits, ranges or timeouts, • force situations to test negative responses, • check all (control) state machine paths, and • force simultaneous control operations from multiple clients. • The ACSI tests focus on the application layer (mapping). • The Device Under Test (DUT) is considered as a black box. The I/O and the communication interface are used for testing. • The test includes testing the versions, data model and configuration file, and the use of applicable ISO 9646 series terminology.

Name	DEF (AUST) 5679 The procurement of computer-based safety critical system
Type	Standard
Group / initiative / organisation	Information Technology Division Defence Science and Technology Organisation
Status	N/A
Publication date	1998
Addressed Industry	Generic
Geographic relevance	Australia
Related standards	N/A
Description	Safety Testing is the activity of experimentation that attempts to reveal errors in the design of a system with respect to a set of safety requirements. Thorough and extensive tests, simulations and trials that do no reveal any violation of safety requirements are an important source of evidence for the Safety Case. Particular forms of safety testing include unit, integration and system tests. Unit and integration tests shall be conducted on individual units, on partially integrated units, and on Components when development is completed. System tests shall be conducted before installation. It is vital that the test data used for safety testing represents a wide and accurate coverage of possible system states and inputs. Safety Test data should be generated from the safety requirements, not from any knowledge of the system design and implementation. The Safety Test team shall include persons that were not closely involved in development of the system. Once a system has been installed, system tests shall be carried out to

	demonstrate the correct implementation of all functional and non-functional requirements. The system tests shall be traceable to safety requirements. The Maintenance of safety critical systems shall be carried out in such a way as to ensure that System Safety Requirements are not violated by any changes made to system software.

Name	NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0
Type	Standards
Group / initiative / organisation	NIST
Status	Special publication
Publication date	2012
Addressed Industry	Energy
Geographic relevance	U.S.
Related standards	IEEE 1815-2010. IEEE 1588. NEMA Smart Grid Standards Publication SG-AMI 1-2009 NAESB WEQ19, REQ18, Energy Usage Informaction NISTIR 7761
Description	Recognizing that some efforts exist today to test products and services based on certain Smart Grid standards, and others are under way, NIST is working with stakeholders and actors through the SGIP to develop and implement an operational framework for interoperability testing and certification that supports, augments, and leverages existing programs wherever practical. To support the accelerated development of an operational framework, NIST initiated and completed the following two major efforts in calendar year 2010: • performed an assessment of existing Smart Grid standards testing programs, • provided high-level guidance for the development of a testing and certification framework. Taking input from NIST, the Smart Grid Testing and Certification Committee (SGTCC) has developed a comprehensive roadmap for developing and implementing the operational framework and related action plans, and has launched a number of focused efforts to develop various documents, tools, and components for the framework. Further development and implementation of the

operational framework by the SGTCC is an ongoing process.

The study was conducted using a set of metrics for an ideal testing and certification program. These metrics are derived from the best practices found among standards testing and certification programs from a variety of organizations both related and unrelated to the power system. The metrics used in the study are:

- Conformance vs. Interoperability vs. Security testing—assessing whether there is a testing and conformity assessment program for a standard that addresses these three areas:
  - whether an implementation conforms to the standard as published—conformance;
  - whether multiple implementations are interoperable with each other—interoperability;
  - whether the implementation correctly makes use of any security features from the standard or other security features available in the device or computer system housing the implementation—security.
- Published test procedures—assessing whether there is a published/publicly reviewed test procedure for the standard;
- Independent test labs—assessing whether there are any independent test labs not operated by product vendors;
- Lab accreditation—assessing whether there is a lab accreditation process for the lab performing the tests (The accreditation could be done by the lab itself or by another entity.);
- Certification/logo—assessing whether there is a certification or logo program for the standard;
- Feedback to standard—assessing whether there is a mechanism to improve the quality of the standard, the test procedures, and/or the operation of the test labs;
- Conformance checklist—assessing whether implementers are provided with a checklist or template in a standardized, published format to indicate what portions of the standard they have implemented;
- Self-certification —assesing wheter it ispossible for the technology providers to self-certify its implementations;
- Reference implementation—assessing whether a reference or “golden” implementation of the standard is available;
- Mature standard—assessing whether the standard is considered as a mature one according to several aspects (e.g., how long it has been published (> 5 years), number of implementations (> 1), mandated (by government, etc.), revisions made, etc.).

Among the stakeholder groups who may find this Release 2.0 document most useful are the following:

- Utilities and suppliers concerned with how best to

	understand and implement the Smart Grid (especially Chapters 3, 4, and 6); • Testing laboratories and certification organizations (especially Chapter 7); • Academia (especially Section 5.5 and Chapter 8); and • Regulators (especially Chapters 1, 4, and 6). New aspects covered: • Developments related to ensuring cybersecurity for the Smart Grid, including a Risk Management Framework to provide guidance on security practices; • A new framework for testing the conformity of devices and systems to be connected to the Smart Grid (the Interoperability Process Reference Manual); • An overview of future areas of work, e.g.,electromagnetic disturbance and interference.

Name	AGA (American Gas Association) 12, Part 1: Cryptographic Protection of SCADA Communications Background, Policies & Test Plan.
Type	Report
Group / initiative / organisation	AGA 12 Task Group
Status	Final
Publication date	2006
Addressed Industry	Generic
Geographic relevance	U.S.
Related standards	AGA 12, Part 2: Retrofit link encryption for asynchronous serial communications AGA 12, Part 3: Protection of networked systems AGA 12, Part 4: Protection embedded in SCADA components
Description	AGA Report No. 12 Part 1 contains the background, security policy fundamentals, and a test plan that apply generally to all areas of cryptographic protection of SCADA systems. AGA 12 Part 1 is intended to serve as a guideline for voluntary implementation of a comprehensive cyber security posture. It focuses on providing background information for improved assessment of a company’s cyber security posture, suggesting policies for a comprehensive cyber security plan and offering a sample test plan for operator implementation. The premise for AGA 12 Part 1 is rooted in the operator’s performance of risk assessment analysis on his/her cyber system. A consistent risk assessment

	analysis equips the operator with the information necessary to understand consequences and formulate an objective business case. Following the performance of a cyber risk assessment analysis, the operator may elect to deploy the encryption methodology that follows in the AGA 12 series of technical reports (i.e., Part 2 and so on). AGA 12 Part 1 is independent of the rest of the AGA 12 series. Compliance with AGA 12 Part 1 does not require compliance with the rest of the AGA 12 series. AGA 12 Part 1 uses cryptographic algorithms approved by NIST and requires FIPS PUB 140-2 compliance. Because cryptography is a sufficiently difficult and subtle area, the AGA 12 Task Group has developed the following path to aid in securing SCADA communications and significantly improving secure access to the maintenance ports of field devices. The scope of AGA 12 Part 1 is to describe the need for SCADA system protection and suggest that an affordable solution may be available. AGA 12, Part 1 proposes steps to define cyber security goals and cyber security practice fundamentals. More significant, AGA 12 Part 1 also defines the cryptographic system requirements and constraints, and cryptographic system test plan applicable to the AGA 12 series. AGA 12 Part 1 serves three purposes: • End users: As an initial step to establishing a cyber security program that defines what is to be protected and all the goals and requirements to protect it. These general requirements should be used to implement, procure, and maintain a SCADA cyber security solution. These requirements necessary for application of the AGA 12 series may be included in the users' procurement specifications. • System integrators: As an initial step to ensuring that SCADA cyber security is specified properly and that the system test plan meets requirements needed to commission the deployed SCADA communication system security solution. • SCADA manufacturers of hardware, software, and firmware: As an initial step to ensuring their product offerings address the needs of the end user for SCADA cyber security.

Name	VDI/VDE 2182
Type	Guideline
Group / initiative / organisation	VDI
Status	Draft
Publication date	2011

Addressed Industry	IT
Geographic relevance	Germany
Related standards	
Description	Guideline VDI/VDE 2182 has been drafted by the "Security" Technical Committee of the VDI/VDE Gesellschaft Mess- und utomatisierungstechnik (GMA), the Society for Measurement and Automatic Control, in collaboration with representatives from the industries which will manufacture and utilize the technology in question, as well as those from higher education and advisory companies. This guideline deals only with IT security. This guideline describes how specific measures can be implemented in order to guarantee the IT security of automated machines and plant; aspects of the automation devices, automation systems, and automation applications used are considered. A uniform, feasible procedure for ensuring IT security throughout the entire life cycle of automation devices, systems, and applications is described, based on common terms and definitions agreed by the vendors of automation devices and systems and their users (e. g., machine vendors, integrators, plant management). The life cycle covers the development, integration, operation, migration, and decommissioning phases. This guideline defines a simple procedure model for the development and description of IT Security. The model consists of eight steps. The implementation of this model from the viewpoint of vendors, integrators/machine vendors and plant management will be exemplary described in the guidelines VDI/VDE 2182 Part 2, Part 3 and Part 4. Applying the methods and measures described in this guideline will allow systematic solutions to be achieved which are appropriate to the level of protection required, meaning that they are also cost-effective.

Name	BSI technical reports
Type	Guideline
Group / initiative / organisation	Federal Office for Informaction Security
Status	
Publication date	2003
Addressed Industry	IT
Geographic relevance	Germany
Related standards	BSI TR-03104 Technical Guideline for production data acquisition, -quality testing and transmission for official documents-

	BSI TR-03105 Conformity Tests for Official Electronic ID Documents BSI TR-03110 Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents BSI TR-03118 Test Specifications for the Technical Guideline for production data acquisition, -quality testing and transmission for passports BSI TR-03121 Technical Guideline Biometrics for Public Sector Applications BSI TR-03122 Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications BSI TR-03125 Preservation of Evidence of Cryptographically Signed Document BSI TR-03126 Technical Guidelines for the Secure Use of RFID BSI TR-03129 PKIs for Machine Readable Travel Documents-Protocols for the Management of Certificates and CRLs BSI TR-03137 Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal) BSI TR-03139 Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Member States BSI TR-03140 Conformity assessment according to the satellite data security act (TR-SatDSiG)
Description	The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry. To minimise or avoid administration or use's risks, the BSI's services are intended for a variety of target groups: it advises manufacturers, distributors andusers of information technology. It also analyses development and trends in information technology. With the publication of Technical Guidelines BSI pursues the objective to spread appropriate IT-security standards. Technical Guidelines address all parties involved in the installation or safeguarding of IT-systems. They complement the technical test specifications of BSI and provide criteria and practices for conformity evaluations ensuring the interoperability of IT-security components as well as the implementation of defined IT-security requirements. Existing standards (e.g. Protection Profiles based on Common Criteria or interoperability standards like ISIS-MTT) are referenced or complemented by Technical Guidelines. On initial release Technical Guidelines merely serve as technical

	recommendations. If referenced by laws or decrees they can become mandatory. Same applies if conformity according to a Technical Guideline is explicitly required as precondition for the participation in public tenders by a official demand carriers. It is possible for manufacturers and distributors to apply for Certification according to Technical Guidelines and have the conformity of their IT-products or -systems confirmed by BSI.

4 Initiatives

4.1 International

Project name	Canadian Cyber Incident Response Centre (CCIRC)
Organisation name	Public Safety Canada
Brief project description	The Canadian government created the Canadian Cyber Incident Response Centre (CCIRC) which aims to ensure the security and resilience of government computer systems, public safety and economic stability of the country. CCIRC is the centre responsible for coordinating services for prevention and mitigation, response and recovery from cyber incidents in government systems. The CCIRC offers expert advice and coordinates the exchange of information between government, critical infrastructure operators, governments and other technology providers. One of the services created by the CCIRC is the test environment for SCADA elements. This service is divided into two test bed models that establish the ability to implement and evaluate different architectures SCADA and security technologies. The models are built in a modular way for modification or expansion, if necessary. With this Test bed environment Canada government aims to improve national security in ICS environments. The CCIRC's functions are (12): • Advice and support to prepare for and mitigate cyber events. CCIRC disseminates various technical and IT manager-focused products that offer guidance, early detection indicators, summary, trend, and operational analysis. Additionally, CCIRC shares technical information on threats, vulnerabilities, risks and incidents with its partners to enhance collective understanding of cyber threats and incidents and help ensure organizations have the information required to make informed decisions. • Technical advice and support to respond to and recover from targeted attacks. CCIRC provides its partners with technical assistance, and performs malware analysis and forensics. In addition to its own expertise, CCIRC can draw on broader Government expertise and resources to help develop

	targeted mitigation and recovery advice. • Access to trusted fora for information sharing and collaboration. CCIRC provides partners access to fora where they can share information within their communities of interest, or more broadly should they wish, and gain access reciprocally to information, expertise and peer support. The CCIRC Community Portal provides a common collaboration tool for organizations that are part of Canada's critical infrastructure sectors. CCIRC uses this portal to share its most recent documents and publications with its partners. In turn, partners have the option of posting documents of their own, and can also use this portal to report cyber incidents to CCIRC.
Period	Since 2007
Country	Canada
Environment	Generic
URL	http://o.canada.com/tag/canadian-cyber-incident-response-centre/

Project name	Idaho National Laboratory (INL)
Organisation name	INL
Brief project description	INL is a science-based, applied engineering national laboratory dedicated to supporting the U.S. Department of Energy's missions in nuclear and energy research, science, and national defense. Its mission is to ensure the nation's energy security with safe, competitive, and sustainable energy systems and unique national and homeland security capabilities. This laboratory is dedicated to research in applied engineering topics in nuclear and energy issues and applied this research to defend the country. In order to ensure energy security of the U.S., the INL has a number of lines of research that can highlight the nuclear security program and support program for NSTB. Since 2004, INL has been a significant contributor to the Department of Energy's broad National SCADA Test Bed (NSTB) program. This national research initiative was developed to help private utilities improve the resilience of control systems associated with energy sector critical infrastructure. Researchers from national laboratories, private industry, and universities collaborate to conduct detailed vulnerability assessments of SCADA systems, communications protocols, and third-party security products. The data collected is used to develop recommended protection strategies for system owners and manufacturers. At INL, full-scale, industry-provided SCADA systems undergo regular cyber analysis by experts widely recognized for securing control systems. The laboratory also conducts onsite assessments and

	training at electricity transmission, generation, and oil and natural gas facilities to better understand real-world installations and provide mitigation strategies to owners and operators. Assessments are backed up by immersive training courses that teach owners and operators about emerging cybersecurity techniques and malware trends. Idaho National Laboratory (INL) produced four reports covering standards in the electric power sector, oil and gas sector, cross-sector, and 13 critical infrastructures identified by the Department of Homeland Security (DHS).
Period	Since 1949
Country	U.S.
Environment	Nuclear energy, electric power sector, oil and gas sector
URL	https://inlportal.inl.gov/

Project name	Japan Center security System Control (CSSC)
Organisation name	Advanced Institute of Science and Technology Azbil Corporation Fuji Electric Co., Ltd. Hitachi, Ltd. Information Technology Promotion Agency McAfee Co.,Ltd. Mitsubishi Heavy Industries Ltd. Mitsubishi Research Institute Inc. Mori Building Co., Ltd. NRI Secure Technologies Ltd. OMRON Corporation The University of Electro-Communications Toshiba Corporation Toyota InfoTechnology Center Co., Ltd. Trend Micro Incorporated Yokogawa Electric Corporation
Brief project description	The CSSC was created in March 2012 and want approach to the successes that have been obtained U.S. in security ICS environments. This initiative plans to develop eight different Test bed systems, including the most common scenarios in Industrial environments that use SCADA elements including substation, power plant, factories, building automation and some sort of gas operations. This

	initiative, in addition to make security Test beds at SCADA devices, has a clear mission to educate stakeholders on issues related to security in industrial environments. Another line that is aimed CSSC is the creation of a security certification for products used in critical systems. In order to ensure the security of control systems of important infrastructure, CSSC conducts various operations thoroughly including R&D, international standardization, certification, human resource development, promotion and security verification of each system. CSSC objectives can be summarized as follows: • R&D of technology to enhance security of control systems • R&D of technology to enhance security of wide-area cooperative systems • R&D of system security verification technology • International collaboration • R&D of control security testbeds CSSC has following 4 task committees working under supervision of the steering committee. The activities of each committee in accordance with its progress are: • R&D and Testbed Task Committee: It sets the direction of R&D regarding control system security as well as the construction of testbeds and promotes R&D and leverages the testbeds. Certification and Standardization • Task Committee: It examines evaluation certification regarding control system security and strategies and policies of standardization. It leverages the testbeds for evaluating certification and standardization. • Incident Handling Task Committee: It prepares for security incidents in control systems and examines the directions of technical development needed for incident handling including the countermeasures of security incidents. • Promotion and Human Resource Development Task Committee: It sets the direction of awareness and human resource development for control system security as a technical research association. It enhances situational awareness and promotes human resource development, making the use of the testbed.
Period	Since 2012
Country	Japan
Environment	Power and gas
URL	http://www.css-center.or.jp/en/index.html

Project name	Mississippi State University SCADA Security Laboratory and Power and Energy Research laboratory
Organisation name	Mississippi State University
Brief project description	This laboratory combines process control systems from multiple critical infrastructure industries to create a testbed with functional physical processes controlled by commercial hardware and software over common industrial control system routable and non-routable networks. The testbed enables a research process in which cybersecurity vulnerabilities are discovered, exploits are used to understand the implications of the vulnerability on controlled physical processes, identified problems are classified by criticality and similarities in type and effect, and finally cybersecurity mitigations are developed and validated against the testbed. The testbed also enables control system security workforce development through integration into the classroom of laboratory exercises, functional demonstrations, and research outcomes. The testbed includes laboratory scale control systems from multiple critical industries including, petrochemical manufacturing, gas pipeline operation, electricity transmission, factory systems, steel manufacturing, and heating ventilating and air conditioning (HVAC) in the form of 7 industrial control systems built with commercially available hardware and software. Each system controls a functional laboratory scale physical process. The physical processes include a storage tank (which models a petroleum storage application), a raised water tower, a factory conveyor belt, a gas pipeline, an industrial blower, and a steel rolling operation, and a smart grid transmission control system. A remote connection exists to a second facility on the university campus which houses electric transmission substation devices and control center software and systems. The electric transmission substation and control center facility contains protection relays, phasor measurement units, phasor data concentrators, a synchrophasor vector processor, programmable logic controllers, a substation GPS clock, a Real Time Digital Simulator, OSISoft PI Historian. The combined testbed is used to support university based research and development in support of identifying existing industrial control system vulnerabilities, developing vulnerability taxonomies to identify common cybersecurity deficiencies in need of solutions development, and to serve as a platform for validating research cybersecurity solutions which serve industry and government. The testbed has been successful in identifying significant vulnerabilities.The combined testbed is also used for pedagogical purposes. First, a graduate course dedicated to industrial control system cybersecurity concepts has been developed. Second, concepts and experiences learned from research activities using the testbed have been integrated into multiple other classes. Finally, researchers are currently developing material for a series of workforce development short courses. (13)

Period	2011
Country	U.S.
Environment	Petrochemical manufacturing, gas pipeline operation, electricity transmission, factory systems, steel manufacturing, heating ventilating and air conditioning
URL	http://www.ece.msstate.edu/

Project name	National SCADA Test Bed (NSTB)
Organisation name	NSTB Multi-Laboratory Team Argonne National Laboratory Idaho National Laboratory Oak Ridge National Laboratory Pacific Northwest National Laboratory Sandia National Laboratories
Brief project description	The National SCADA Test Bed Program is a national resource to help secure the nation's energy control systems. It combines state-of-the-art operational system testing facilities with research, development, and training to discover and address critical security vulnerabilities and threats the energy sector faces. This U.S. initiative is one of the most active and known to exist in the field of international Test beds, was the U.S. Department of Energy (DOE) who established the National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) program to create a partnership between industry and the U.S. government to improve the safety of ICS environments. Creation of the NSTB was funded by DOE Office of Electricity Delivery and Energy Reliability (DOE-OE) and doing the work together Idaho National Laboratory (INL) and Sandia National Laboratories (SLN). In addition to these, it also participate Pacific Northwest National Laboratory, Argonne National Laboratory, National Institute of Standards and Technology. These laboratories have joined together to address the challenges that appear in the ICS security environments in the energy sector. To find a solution they perform research and work based on: • Control systems testing, research and development; • Advanced technology development; • Control systems requirements development; • Industry outreach. The main objective of NSTB is to share information obtained in the tests performed with the parties involved in security issues. The NSTB works directly with manufacturers of products and solutions as the information it obtains from its information security assessments is really sensitive. Another objective of this initiative is the

	development of methodologies for disclosure without affecting commercially stakeholders (manufacturers, users...), to distribute sensitive information the NTSB always ask permission. As for the objectives NTSB seeks in its safety analysis ICS environments are the following: • Evaluation of control systems and components that make ICS environments, performing tests in controlled environments such as the Test bed • Specific training, describing the use of security models, explaining the vulnerabilities found and methods for their mitigation. • Share information in a way that can be used by the general public, even to be made from this information SCADA security standards. The National SCADA Test Bed provides a variety of realistic testing environments to help industry and government identify and correct vulnerabilities in control systems including SCADA, EMS (Energy Management Systems) and DCS. It includes several testing facilities.
Period	Since 2003
Country	U.S.
Environment	Electricity, oil, and gas industries.
URL	http://energy.gov/oe/national-scada-test-bed

Project name	Sandia labs
Organisation name	Sandia Corporation
Brief project description	The Sandia National Laboratories, are two major United States Department of Energy research and development national laboratories which have been investigating in security environments over 60 years. Their primary mission is to develop, engineer, and test the non-nuclear components of nuclear weapons. The main work of this laboratory is to work as a subcontractor for the U.S. government, under contract with the Department of Energy's National Nuclear Security Administration (NNSA), actively participating in the implementation of laws and standards for the security of companies and organizations operating within the United States. SNDLab has created an organization with several lines of research for the security of control systems ranging from autonomous agent systems applied to SCADA, a cryptographic security, system evaluation, and red team activities. As a multidisciplinary national laboratory, Sandia accomplishes tasks integral to the mission and operation of its sponsoring agency by ensuring the following:

	• Anticipating and resolving emerging national security challenges; • Innovating and discovering new technologies to strengthen the nation's technological superiority; • Creating value through products and services that solve important national security challenges; • Informing the national debate where technology policy is critical to preserving security and freedom throughout our world.
Period	Since 1948
Country	U.S.
Environment	Generic
URL	http://www.sandia.gov/

Project name	Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project
Organisation name	University of Illinois Dartmouth College Cornell University University of California Washington State University (Support from the Department of Homeland Security)
Brief project description	TCIPG is the successor to the TCIP Center and TCIPG's research plan is focused on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, and/or power emergencies. The main goals of this project are (14): • Provide for experimental support/integration of TCIPG projects. Provide a simulation and emulation environment with real hardware and software used in the power grid. • Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems. • Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities. The research plan of TCIPG can be explained in four steps: • Develop new modeling and evaluation technologies to enhance evaluation capabilities of the testbed. • Continue to expand the equipment capabilities, features, and functionality through strategic integration of both

software and hardware.

- Develop integration glue to seamlessly integrate power grid equipment and software into the testbed by coupling simulation, emulation, and real equipment.
- Leverage existing and emerging research from other areas when it can benefit the testbed effort.

The impact is being made at all levels in the project. At the device level, attested meters have been developed that provide the advanced features needed for energy control, while ensuring appropriate access control and also preserving customer privacy. Hardware support has been developed to support application-aware detection and recovery mechanisms in power system devices. Likewise, secure co-processors have been developed to perform efficient cryptographic computations to facilitate communications between substations and control centers on the grid. At the network level, protocols are being developed to provide efficient, timely, and secure publishing of and subscription to process control system data; to support secure and timely data and resource aggregation in process control systems; and to provide federated identity management, access management, and trust negotiation for the grid. These protocols are being designed with next-generation communication and control requirements in mind, providing the building blocks for a more robust, secure, timely, and adaptive grid infrastructure. Finally, a combined simulation/testbed environment has been developed that mimics specific aspects of the IT infrastructure of the power grid accurately, while being scalable. Together, these innovations provide clear directions toward a next-generation IT infrastructure for the power grid that is reliable, timely, and secure, supporting the continuous functioning of the nation's electric power infrastructure.

The TCIPG research results are summarized in three points:

- Real-time Immersive Network Simulation Environment (RINSE): large-scale network simulation.
- Virtual Power System Testbed: cyber/physical coupling of simulation, emulation, and real equipment.
- Network Access Policy Tool (NetAPT): policy tool to evaluate network access paths and verify compliance with a global policy.

And the uses cases are:

- Provide a multi-faceted approach to security through testbeds, education and training, field testing, and tool creation.
- Facilitate collaboration among researchers and industry to work towards creation ofmore resilient critical infrastructure.
- Facilitate rapid transition and adoption of research by industry.

	• Provide positive real-world impact through engagement. Finally TCIPG has also developed interactive and open-ended applets for middle-school students, along with activity materials and teacher guides to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students.
Period	Since 2010
Country	U.S.
Environment	Energy
URL	http://tcipg.org

Project name	ICS SandBox
Organisation name	Natural Sciences and Engineering Research Council of Canada (NSERC).
Brief project description	Companies operating in the oil and gas industry have at their disposal a SCADA security test laboratory for testing the impact of cyberattacks on their systems. The so-called Industrial Control System (ICS) Sandbox, based in Montreal, aims at simulating the real threats to critical infrastructure and finding ways to block them in real time. ICS Sandbox is funded by Natural Sciences and Engineering Research Council of Canada (NSERC). The laboratory includes 100 machines - servers, workstations, PLCs, sensors, electrical simulators, and commercial SCADA software. Representatives from academia, the power industry, and security vendor world have teamed up to offer the testbed environment to critical infrastructure operators in the U.S. and Canada, as well as Brazil, where a similar testbed is now under construction. The testbeds ultimately will be expanded to support other sectors of critical infrastructure. The ICS Sandbox can also be used to test out patches to SCADA products.
Period	Since 2007
Country	CA
Environment	Oil and Gas
URL	http://www.darkreading.com/vulnerability/scada-sandbox-tests-real-world-impact-of/240149728

Project name	TRUST-SCADA Experimental Testbed
Organisation name	TRUST (Team for Resarch in Ubiquitous Secure Technology)
Brief project	The TRUST SCADA Testbed is an affordable software-hardware

description	infrastructure that supports experimentation with systems-level security technologies for SCADA systems. The testbed, in its current implementation, consists of: • A realistic plant simulator, which uses Simulink/Stateflow dynamic system models for real-time simulation of physical plants (e.g., chemical manufacturing processes, power generation and distribution systems, oil refineries), • Low-cost SCADA RTU emulator boards that run low-level regulator/SCADA software and are connected to the plant simulator, and • Affordable, networked SCADA host emulator boards that could run higher-level control and optimization algorithms which provide setpoints and control commands to the RTU emulators. The TRUST-SCADA Testbed Goals are (15): • Assess vulnerabilities of current SCADA implementations in realistic settings • Provide and test solutions to address such vulnerabilities • Test innovative architectural and technological solutions for next generation SCADA • - Provide an open-source design for an affordable, and highly flexible testbed for the TRUST community The SCADA Testbed Requirements • Modularity: Must be able to model several SCADA elements like processes, network awchitectures and communicatons topologies, media and protocols. • Reconfigurability: Needs to be easily reconfigurable to test new control schemes, attack scenarios, solutions • Remote access: Should be available to remote users • Accurate modeling: Should be a realistic model of a real world process
Period	2008-2013
Country	U.S.
Environment	Generic
URL	http://www.truststc.org/

Project name	Industrial Instrumentation Process Lab
Organisation name	BCIT (British Columbia Institute of Technology)
Brief project description	The BCIT Industrial Instrumentation Process Laboratory is located on the Burnaby campus. This facility houses a fully operational distillation column, IIPL evaporator and power boiler. The ability to create variety of complex control processes is key

	feature of BCIT's industrial laboratory facilities. For example, the following industrial processes are available for control and security research: • A highly-instrumented glycol evaporator and complementary distillation column presents challenging control problems for any control design strategy. It provides an excellent test bed for interfacing multiple vendor equipment with ease. Multiple computer stations and an array of interfacing options allow users to create custom equipment configurations with a minimum of difficulty. • Four vapour/liquid heat exchangers monitored with state-of-the-art Foundation Fieldbus instrumentation and final control equipment. This facility has proved invaluable in the development of commercially successful predictive/adaptive advanced control software by highlighting design flaws that were undetectable with computer simulation models. • A fully functional batch pulp digester with supporting instrumentation and control equipment. This facility, used in the training of pulp and paper technology students and for industry-sponsored training, is readily adaptable and configurable. An advanced control algorithm provides the opportunity to experiment with and develop optimum digesting parameters. • Chemical Blending / Reaction Process - this unique chemical blending line is yet another example of the diversity of process and equipment readily accessible for research and development purposes.
Period	
Country	CA
Environment	Generic
URL	http://www.bcit.ca/appliedresearch/tc/facilities/industrial.shtml

Project name	Viking project
Organisation name	ABB AG E.ON AG EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZURICH MML ANALYS & STRATEGI AB The University System of Maryland Foundation, inc. Kungliga Tekniska Hoegskolan Astron Informatikai Fejleszto es Tanacsado KORLATOLT FELELOSSEGU TARSASAG
Brief project	The VIKING project will concentrate its research on computerized

description	system for the supervision and control of electrical transmission and distribution networks. One of the reasons to limit the project to the electrical process is that the results of VIKING is believed to be applicable to other SCADA systems used for other critical infrastructures like gas, water, telecommunication, etc. and, as described in the Introduction, the vital importance of the electricity supply. The objective of the VIKING project is to develop, test and evaluate methodologies for the analysis, design and operation of resilient and secure industrial control systems for critical infrastructures. Methodologies will be developed with a particular focus on increased robustness of the control system. As mentioned, the focus is on power transmission and distribution networks. The project combines a holistic management perspective—in order to counteract sub-optimization in the design—with in-depth analysis and development of security solutions adapted to the specific requirements of networked control systems. The traditional approach to verify the security of SCADA systems has been ad-hoc testing of existing commercial SCADA system in laboratory environments. The systems to be examined have been installed in different labs and tested by skillful people searching for cyber attacks vulnerabilities. The focus in these tests has been on the protection of the central computer system of the SCADA system, since the central computer system has most connections to the outside world through office networks, vendor links and Internet. The VIKING project takes an alternative and complementary approach to SCADA system security. Firstly, it studiesthe whole control system from the measurement points in the process itself over the communication network to the central computer system. . Secondly, and more importantly, it takes a model-based approach to investigating SCADA system vulnerability. Models are defined for the SCADA system, for the electrical process as well as of for the society that is dependent on the electricity supply. The society models are used to evaluate the economic consequences coming from disturbances in the electricity supply and to give load scenarios for the simulations. The power system models are in turn used to evaluate the effects on the electricity supply caused by SCADA system misbehavior. Finally, SCADA system architectural and cyber-physical models are employed to assess the effect on SCADA system behavior caused by cyber attacks. Based on analysis performed on these models, VIKING proposes mitigation actions to be taken to decrease or to eliminate these risks. The results of the project are evaluated on a test-bed that can be configured to simulate cyber attacks on the power network coming from SCADA and the corresponding consequences in the virtual society. The results of VIKING project are: • Estimates of the security risk (in terms of monetory loss for the society) based on threats trees, graphical system architecture and society models

	- Comparable, quantitative metrics for cyber security for different control system solutions - Help with identifying ”weak spots” and how to mitigate the - An environment for performing what-if analyses of the security risk impact of different architecture solutions - Use of process knowlege as an application level Intrusion Detection Systems to detect manipulation of data - Use of existing and new communication solutions to increase security in power system communication Finally, the objectives of the testbed are: - Provide a holistic framework for identification and assessment of vulnerabilities for SCADA systems. - Provide a reference model of potential consequences of misbehaving control systems in the power transmission and distribution network that can be used as a base for evaluating control system design solutions. - Develop and demonstrate new technical security and robustness solutions able to meet the specific operational requirements that are posed on control systems for our target area. - Increase the awareness of the dependencies and vulnerabilities of cyber-physical systems in the power industry.
Period	Since 2008
Country	U.S. / SE
Environment	Energy
URL	http://control.ee.ethz.ch/~viking/

Project name	DETER project
Organisation name	U.S. Department of Homeland Security Science and Technology
Brief project description	DETER is both a research project, and the operator of DeterLab, the leading cyber-security experimentation lab for researchers worldwide. DETER’s mission is to significantly increase the scale, pace and power of cyber-security research for homeland security and critical infrastructure protection. Their goal is to accelerate the development of effective, innovative cyber-defense technology by advancing the state of cyber-security experimentation and science. Their twofold approach is based on both their research, and the efforts of cyber-security scientists and technologists who use DeterLab as a scientific facility for cyber-defense invention and evaluation. In their research program we develop novel methods, technology and infrastructure for cyber-security experimenters to employ in creating and testing new security technologies. Their

	research results are put into practice in DeterLab, where members of their research community - spanning over 150 institutions from a dozen countries - use their advanced experimentation facilities. DeterLab provides unique, real-world capability to research, develop, discover, experiment on and test cyber-defense technology. Approved users can access DETER's advanced resources and tools, and perform the repeated, verifiable experiments that are critical to true scientific research. With research, DeterLab operation, education, and community support, DETER seeks to transform cyber security research into a rigorous experimental science, by creating the advances in methods and technologies for verifiable experiments in a realistic test environment, and by making those advances widely available to foster rapid growth in research activity and results. In practice in DeterLab, DETER enables experimenters to share data, lab set-up, software and tools, experimental procedures, results, and other information that should enable new experimenters to stand on their predecessors' shoulders, rather than start at ground level for every new project.
Period	Since 2003
Country	U.S.
Environment	Generic
URL	http://deter-project.org/

Project name	The Virtual Power System Testbed (VPST) and Inter-Testbed Integration
Organisation name	University of Illinois
Brief project description	The Virtual Power System Testbed (VPST) is part of the Trustworthy Cyber Infrastructure for the Power Grid (TCIP) and is maintained by members of the Information Trust Institute (ITI). VPST is designed to be integrated with other testbeds across the country to explore performance and security of Supervisory Control And Data Acquisition (SCADA) protocols and equipment. They discuss potential use cases in order to motivate the integration of VPST with other testbeds, identify requirements of interconnected testbeds, and describe our design for integration with VPST. As part of the NSF/DOE/DHS supported TCIP project, VPST combines large-scale simulation/emulation of networks of SCADA power devices with real power system hardware and software, and a commercial electric flow generation and distribution simulator. VPST is unique in its integration of virtual and physical equipment. VPST's principal role so far has been to demonstrate the feasibility of integrating the components it has, the feasibility of a number of cyber-attacks, and studies of performance and effectiveness of

	certain other TCIP developed technologies. It is not yet to the level of general purpose utility achieved by DETER, although they are working to bring it to that state. They have redesigned the VPST architecture to support integration with other testbeds, and have already demonstrated basic integrative functionality. They aim towards enabling one to leverage resources from external collaborators and accomplish tasks that may not have been feasible without them. For example, one lab may have expertise in cyber warfare and another may emphasize actual SCADA devices. VPST provides detailed models of SCADA-specific protocols, enabling studies where an attack is mounted on a large-scale SCADA network. Such integration has a unique set of requirements, and they have extended VPST with these in mind. VPST is divided into three main subsystems: • VPST-E handles electrical simulation. The primary component is PowerWorld which is capable of simulating large scale electrical networks at the bus level. They use this to model city-sized or larger power grids. • VPST-C handles network simulation based on RINSE, which provides a highly scalable virtual network that is used to model the cyber domain of the electrical grid. • - VPST-R-local represents all the real devices. Any software that is run rather than simulated resides on some real device in the VPST-R-local, and is represented inside of VPST-C by a device proxy. Devices in VPST-R local are capable of interacting with VPST-E through a converter, and VPST-C through its emulation capability.
Period	
Country	U.S.
Environment	Enregy
URL	

Project name	Virtual Control System Environment (VCSE)
Organisation name	Sandia National Laboratories
Brief project description	The Virtual Control System Environment (VCSE) is a modeling and simulation environment that bridges the gap between control system models and process simulation. Tools and techniques exist for simulating and emulating control system field devices, but results from the security analysis these tools currently support are limited because the physical processes being controlled are not included. Leveraging Sandia's proven Umbra modeling environment, the VCSE intertwines the device and process simulations to provide an integrated system capable of representing realistic responses in the physical process as events occur in the control system and vice versa.

	The VCSE is comprised of simulated control system devices, such as remote terminal units (RTUs), programmable logic controllers (PLCs) and protection relays, and simulated processes, such as electric power transmission systems, refinery processes, and pipelines. The simulated control system devices are capable of communicating over Internet Protocol (IP) networks using standard Supervisory Control and Data Acquisition (SCADA) protocols like Modbus and DNP3. The VCSE also includes support for hardware-in-the-loop, wherein real field devices under study (i.e. a specific model of PLC) can be connected to and interact with the physical process being simulated. The VCSE provides a means for creating large-scale control system test environments suitable for cyber security experiments. Leveraging modeling and simulation, the test environments can be scripted to suite each experiment as necessary, are repeatable, and are much cheaper to construct than real or even labscale test environments. The use of standards-based SCADA protocols in the simulated field devices also means 3rd party ICS and cyber security testing applications can still be used, and supports the use of simulated and emulated network environments as well. The VCSE provides an analysis capability that supports assessing and improving the cyber security of control systems used in the energy sector as described by The Roadmap to Secure Control Systems in the Energy Sector. The VCSE provides an environment where hardware and software upgrades and new mitigations can be evaluated before installation in an operational environment.
Period	Since 2009
Country	U.S.
Environment	Energy
URL	http://www.sandia.gov/ccd/projects.html

Project name	Illinois Center for smarter electric grid (ICSEG)
Organisation name	Information Trust Institute (University of Illinois)
Brief project description	The Illinois Center for a Smarter Electric Grid (ICSEG) is a 5-year project that is developing and operating a facility at the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign to provide services for the validation of information technology and control aspects of Smart Grid systems, including micro grids and distributed energy resources. The key objective is to test and validate within a laboratory setting how new and more cost-effective Smart Grid technologies, tools, techniques, and system configurations can be used in trustworthy configurations that significantly improve upon the ones that are in common practice today. The laboratory is becoming a resource for Smart Grid equipment suppliers and integrators and electric utilities to allow

	validation of system designs before deployment.
Period	
Country	U.S.
Environment	Energy
URL	http://www.iti.illinois.edu/research/power-grid/illinois-center-smarter-electric-grid

Project name	EMIST Project
Organisation name	NSF DHS DARPA
Brief project description	The Evaluation Methods for Internet Security Technology (EMIST) project was a collaboration among the organizations with the first wave of research users of the DETER testbed, which has since evolved into DeterLab. Starting in March 2004, EMIST was funded by NSF, DHS, and DARPA to pursue cyber-security research with the testbed, and to collabroate with the DETER project on the development of testbed capabilities -- in essence, the first user group, working closely with DETER to project feedback on testbed capabilities as DETER built and operated the testbed as experimental infrastructure for EMIST and other security researchers. The EMIST team of researchers were from Penn State, UC Davis, Purdue, ICSI, McAfee, Sparta, and SRI, and included experts in security, networking, data analysis, software engineering, and operating systems, all committed to developing testing frameworks and methodologies for cyber security. The general objective of EMIST was to develop thorough, realistic, and scientifically rigorous testing frameworks and methodologies for particular classes of network attacks and defense mechanisms. These testing frameworks were adapted for different kinds of experimental approaches, including simulators such as NS, emulation facilities such as the DETER testbed, and both small and large testbeds of real hardware, including: attack scenarios; attack simulators; generators for topology and background traffic; data sets derived from live traffic; and tools to monitor and summarize test results. These frameworks allowed researchers to experiment with a variety of parameters representing the network environment, attack behaviors, and the configuration of the mechanisms under test conditions. These frameworks and methodologies were being validated through experiments on the DETER testbed. The validation involved tests on representative network defense mechanisms, including intrusion detection systems (IDSs), automated attack traceback mechanisms,

	traffic rate-limiting to control DDoS attacks, and mechanisms to detect large-scale worm attacks. DDOS, worms, and routing security had distint research teams working on projects within EMIST.
Period	2004 - 2007
Country	U.S.
Environment	Generic
URL	http://deter-project.org/emist

Project name	The Critical Infrastructure Test Range (CITR) Program
Organisation name	
Brief project description	CITR Program was established at the Idaho National Laboratory (INL) to fulfill the needs and objectives defined by the U.S. Department of Energy (DOE) Office of Energy Assurance and the National Strategy for Homeland Security. The CITR was established to support the testing and evaluation needs of DOE, the Department of Homeland Security, the Department of Defense, first responders, and other clients. The primary goal of the CITR Program is to establish the necessary resources, including facilities, equipment, protocols, and personnel, to provide a national testing capability for evaluating the vulnerabilities inherent in Supervisory Control and Data Acquisition (SCADA) and control systems. The CITR has the capability to test, at near full-scale, the protective measures of the nation's critical infrastructure at a system-level, thereby providing independent verification and validation of homeland security systems. INL will use the knowledge gleaned from these tests to support development of critical infrastructure standards and certification procedures and ensure that new infrastructures and components being integrated into the existing infrastructures do not introduce new vulnerabilities into those systems. This approach will allow us to identify SCADA and control system vulnerabilities, fix existing national vulnerabilities by developing defensive procedures for existing infrastructures, and design and construct the more attack resistant smart infrastructures of the future. The CITR consists of the following specialized critical infrastructure test beds, facilities, and resources: • The SCADA/control system test bed, which has been used to test a representative SCADA system for vulnerabilities found in the operating system of that SCADA system • A cyber security test bed • An enhanced communications test bed • The INL power grid, which was evaluated to determine its potential use as a test bed

	• Various existing INL site facilities and buildings located approximately 50 miles west of Idaho Falls, Idaho • A specialized data acquisition system, which was designed and built for use during testing of physical security systems and components.
Period	2005
Country	U.S.
Environment	General
URL	

4.2 European

Project name	CRUTIAL (Critical Utility InfrastructurAL resilience) project
Organisation name	CESI RICERCA Faculty of Sciences of the University of Lisboa CNR-ISTI LAAS K.U.Leuven CNIT
Brief project description	CRUTIAL addresses new networked ICT systems for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intranets), which are in turn connected to the Internet. CRUTIAL's innovative approach resides in modelling interdependent infrastructures taking into account the multiple dimensions of interdependencies, and attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks. The objectives of the project are: • Investigation of models and architectures that cope with the scenario of openness, heterogeneity and evolvability endured by electrical utilities infrastructures; • Analysis of critical scenarios in which faults in the information infrastructure provoke serious impacts on the controlled electric power infrastructure; • Investigation of distributed architectures enabling dependable control and management of the power grid. The project will: • Identify and describe control system scenarios; • Provide modelling approaches for understanding and mastering the various interdependencies;

- Develop a test bed integrating the electric power system and the information infrastructure;
- Investigate fault-tolerant architectural configurations;
- Provide qualitative and quantitative support for the identification, analysis and evaluation of the scenarios identified. The results will be validated against test beds of Electric Power Systems.

The project's results will help in designing and assessing new Electric Power systems and information infrastructures. Thus, they will enable to reduce the current (unfortunately repetitive) blackouts, in terms of frequency, duration and extent, and provide insights to Electric Power companies and standardization bodies for exploiting resilience in critical utilities infrastructures.

CRUTIAL has been planned in 7 workpackages, five of which are technical workpackages. The five technical workpackages adequately reflect how the project will organise the research, while WP6 deals with dissemination and WP7 with management activities, respectively:

- **WP1: Identification and description of control system scenarios**
  The goal of WP1 is the identification of reference Control System Scenarios from the application domain and their description in a notation suitable for modelling them in later work packages.
- **WP2: Interdependencies modelling**
  The objective of WP2 is to define a conceptual modelling framework that is well suited
- **WP3: Testbed development**
  The goal of WP3 is to design and implement two testbeds, integrating the electric power system and the information infrastructure. The detailed objectives are threefold:
  - elaboration of control scenarios in order to better identify them (related to WP1);
  - elaboration of architectural patterns (related to WP4);
  - elaboration of interdependencies, complementary to the modelling of WP3.

  The testbeds are composed of two platforms: the first will be based on power electronic converters that are controlled from PCs that are interconnected over an open communication network (Herakles, at K.U.Leuven); whilst the latter will consist of power station controllers on a real-time control network, interconnected to corporate and control centre networks (at CESI).
- **WP4: Architectural solutions**
  The aim of WP4 is to define and investigate architectural configurations that induce prevention of more severe faults and tolerance of the remaining faults on the various

	information infrastructures (e.g., monitoring & control, management) that interact on a decentralized power grid. - **WP5: Analysis and evaluation of control system scenarios** The overall goal of WP5 is to provide qualitative and quantitative support for the identification, the analysis and the evaluation of the control system scenarios identified in WP1 and applied in the testbeds of WP3, and enriched in their architectural solution by the work done in WP4.
Period	Since 2006
Country	IT
Environment	Energy
URL	http://crutial.rse-web.it/

Project name	ENEA Test Bed
Organisation name	Safeguard EU-Project
Brief project description	The SCADA Test Bed available at ENEA, mainly developed for the Safeguard European Union Project purposes, was built taking into account two layers: - The physical layer, namely the electrical grid; - The cyber control layer, namely the distributed SCADA system. The electrical grid is simulated by the E-AGORA electrical load flow simulator, made available by the owner (AIA) to the other partners of the Safeguard Consortium. E-AGORA calculates the load flow of an electrical network model, under all system conditions, even when the system is close to voltage collapse. It employs a very advanced algorithm that uses Newton-Raphson iterative mathematics, the same algorithm and methodology used in the real-time application. The application allows the user to visualize the load flow data (system bus voltages, power flow) and to perform actions such as opening and closing switches, changing system bus voltages, electrical parameters and generators settings. It also includes a two-dimensional representation of the electrical system and provides editing capabilities. The electricity network chosen for testing Safeguard agents it is the test network published by IEEE. The E-AGORA simulator does not allow a dynamic simulation of the electrical network. In other words, it is not possible to see the continuous evolution of the electrical network due to the continuous variation of the loads, but after a first load flow calculation, the user is responsible for manually changing the loads and then requesting again a new load flow evaluation. This missing feature has been covered by ENEA by developing an interface module, the Analog-Digital (AD) component, in charge of regularly updating load data and requesting power flow calculations. Therefore it is possible to

follow the standard network evolution during a complete day, week, season or any time interval.

The ENEA's planned facilities in the Cybersecurity field include an improved SCADA test bed, which allows:

- To plug SCADA provided by different vendors (HW and SW)
- To simulate different power grids
- To plug add-on new modules for improving CI resilience

Activities performed in the test bed:

- To identify vulnerabilities and threats of SCADA currently employed by different operators
- To understand the impact of SCADA vulnerabilities on the power grid
- To identify, test and demonstrate algorithms and tools aimed at improving CIs resilience
- To Benchmark different algorithms and solutions

Regarding Modeling and Simulation in SCADA Cybersecurity, Institutional Tasks and Research Objectives are presented:

Institunional Tasks:

- To increase the Italian governmental bodies and stakeholders awareness about interdependency modeling and simulation issues
- To foster collaboration and joint activities on interdependency modeling and simulation issues within Italy - To find suitable solutions to manage with this issue

Research Objectives:

- Assessment of threats, vulnerabilities and resilience of SCADA
- Early detection of attacks throught new technological solutions
- Implementation of a Test Facility for SCADA Cybersecurity

Regarding information exange, Institutional Tasks and Research Objectives are another ones:

- Institutional Tasks:
  - To increase stakeholders' awareness about the importance of Information Exchange and Public Private Partnership (PPP)
  - To foster collaboration of this topic with/between stakeholders
  - To find suitable solutions to manage with this issue
- Research Objectives:
  - Modeling the Information Exchange in a trusted way
  - Develop the appropriate technology supporting Information Exchange
  - Improving situational awareness and mutual

	coordination among CIs operators • Implement a Test Facility for Information Exchange
Period	Since 2009
Country	IT
Environment	Energy
URL	http://www.infrastrutturecritiche.it

Project name	European Network for Cyber Security (ENCS)
Organisation name	Alliander KPN DNV KEMA TNO Radboud University Nijmegen
Brief project description	The European Network for Cyber Security has developed a project aimed at the elaboration of a test bed that is responsible for checking the security level in ICS environments. The project develops a model of evidence for the use of ICT technologies in critical infrastructure environments; this is done by testing the systems thus improving the resistance of these critical environments on cybersecurity. ENCS has a number of systems, both physical and virtual security testing of various devices and / or systems. This behaviour is checked in an environment very similar to the real. The mission of ENCS is to improve the resilience of European critical infrastructures. ENCS' initial objective is to raise the cyber security bar for the electricity supply. ENCS works with dedicated resources on research & development, testing, monitoring, education & training and information & knowledge sharing. In addition it uses ENCS network in government, academia and business to provide: • Applied research, demand driven, tailored to DSOs • Information & Knowledge sharing (including participation in experts-, standardization groups & ISAC) • End-to-end security test e.g. conformity testing, vulnerability assessment, penetration test, security code review • Web based cyber security awareness course • Red Blue Team training • Class room training • Risk assessment • Security assessment • Develop & evaluate security requirements • Monitoring solution for ICS-Scada & smart grids, including network scanning and visualization

	ENCS offers a test environment where end-to-end cyber security can be tested. The testing can take place either in a well-prepared laboratory simulating the utilities infrastructure, or using the physical infrastructure of the utility itself. The testing service line will conduct end-to-end security (system) testing (from idea/request to reporting). ENCS will then provide advice on how to mitigate the vulnerabilities found and raise the quality level of prevention. ENCS offers a unique opportunity for researchers to execute their programs in a medium and low voltage grid environment. This is the closest real-world grid test environment before going into production. Projects using the ENCS lab environment can add value to results by using live grids. In contrast to desk studies, live operating circumstances create a mindset very close to reality. This is mainly due to many operational variables in live grids that can ‘feed’ complex research models and offer new insights, specifically for security research projects. ENCS programs can make use of this knowledge to investigate operational processes, which are an important part of security. ENCS offers: • The organization, processes and facilitation for ENCS security research and testing on ICS systems, field equipment, communications and smart meter infrastructures. • Installed base with live medium and low voltage grid conditions. • Environment for innovative privacy and security development. • Knowledge center for smart grid and smart meter test & research in an international network. • Vulnerability assessments and penetration testing.
Period	2012-2013
Country	NL
Environment	Generic
URL	https://www.encs.eu/

Project name	European Network of Secure Test Centres for Reliable ICT-controlled Critical Energy Infrastructures (ESTEC)
Organisation name	European Commission (EC)
Brief project description	The ESTEC project "European Network of Centres for Reliable Secure Test ICT-controlled Critical Energy Infrastructures" is an initiative funded by the European Union and managed by the DG-JLS, which is placed under the European Programme for Critical Infrastructure Protection (EPCIP). The project based its efforts on gathering information on the methodology of attacks and how they

	confronting these attacks from SCADA devices, and the generation of a methodology to test the operation at European level. The objective is support the European Union on security in ICS environments, allowing their results make European directives to identify and designate the critical infrastructure types existing in all member countries. The project will also carry out an identification of vulnerabilities in SCADA devices, forming alerts on these devices and secure defining requirements, good practice guides and security policies ICS environments. The purpose of ESTEC is to evaluate vulnerabilities that exist in SCADA systems through testing in controlled environments. Such tests are performed to identify possible effects that may occur in critical environments. The need for the environments in which they test be as close to reality, makes the project has to have a hardware infrastructure as similar to the real and simulation environment for software advanced enough required to create scenarios. For the accomplishment of security testing carried out in this project, different test centres have been developed, which are divided by sector. These centres consider different configurations of the devices in different configurations. ESTEC project define test bed areas divisions as follows: • Energy Test Centre, including SCADA and DCS Test; • Electricity Transmission and Distribution Test Centre; • Electricity Production Test Centre; • Oil Transmission and Distribution Test Centre; • Oil & Gas Production Test Centre; • Communication Network Test Centre; The main goal of the ESTEC would be to assess SCADA systems vulnerabilities by testing them in a fully operational environment, i.e. when connected to energy Critical Infrastructures. As this cannot be done on real infrastructures without taking safety and security risks, the ESTEC should include the reproduction of real infrastructures (Test Range) or a platform simulating its behaviour (Test Bed). Such reproductions/simulations can be very useful also for other tasks, such as the assessment of countermeasures. In fact, main security solutions are derived from the ICT sector (holding security priorities that are very different from SCADA systems', and thus their use on SCADA systems has to be carefully tested not only to prove their effectiveness, but also their compatibility with nominal Critical Infrastructures behaviour.
Period	2008
Country	BE
Environment	Energy
URL	http://www.estec-project.eu/

Project name	European Reference Network for Critical Infrastructure Protection (ERNCIP)
Organisation name	European Commision Joint Research Centre
Brief project description	ERNCIP aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards. ERNCIP's mission is to foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities. ERNCIP is a direct response to the lack of harmonised EU-wide testing or certification for CIP products and services, which is a barrier to future development and market acceptance of security solutions. The ERNCIP Office operates within the organisational framework of the Institute for the Protection and Security of the Citizen (IPSC) of the European Commission's Joint Research Centre. The Institute provides scientific and technological support to European Union policies in different areas, including global stability and security, crisis management, maritime and fisheries policies and the protection of critical infrastructures. IPSC works in close collaboration with research centres, universities, private companies and international organisations in a concerted effort to develop research-based solutions for the security and protection of citizens. The ERNCIP Office has been mandated by Directorate General Home Affairs (DG HOME) of the European Commission. ERNCIP Strategic Goals are (16): • Improve the protection of critical infrastructure in the EU • Support the development of a single EU market for security products • Identify gaps in EU security product testing capabilities ERNCIP has different thematics groups who could: • Promote sharing of information, good practice and experimental results across all CIP stakeholders; • Harmonise test protocols; • Promote standardisation of test methods; • Recommend EU-wide evaluation / certification / labelling procedures; • Recommend new areas for research and investment. ERNCIP's general activities are:

	• Management, coordination and administration; • Thematic area prioritization, supervision and promotion; • Develop and operate ERNCIP Inventory; • Legal-regulatory, policies and security ERNCIP performed its first conference and the conclusions of it were: • The conference discussions underlined the importance of testing security solutions and offered a number of practical suggestions, such as: • more testing capabilities should be developed • investment is required to improve the lab capabilities and availability in the EU. Future ERNCIP activities could include: • Support to the pre-commercial procurement process in security. • Technology assessment • Scenario-based process evaluation • Guiding manufacturers on how to obtain EU-wide certificates • More support for labs • Experiments, benchmarks • Training.
Period	Since 2009
Country	IT
Environment	Generic
URL	http://ipsc.jrc.ec.europa.eu

Project name	JRC Test Bed
Organisation name	JRC
Brief project description	In 2006, the JRC developed the first laboratory in Europe for the ICT security test and analysis of power plants. The Test Centre consists on the emulation of a power plan section, and of a network which includes the following subsystems (17): • The Process Network: including the process SCADA; • The Diagnostic Systems: used to analyze the anomalies possibly detected in the functioning of the power plant; • The Control Network: used to deliver control commands and data to and for the Process Network (which groups together the SCADA and the diagnostic systems); • The Data Network: used to deliver special control flows among the different power plants; • The Company Intranet: based on a typical Windows domain architecture, is used to deploy business services such as the

	interconnections between the administrative and the technical company areas, access to production information, maintenance data, etc.; • The Process Firewall between the Data Network, Process Network, DMZ Network and the Intranet: used to guarantee access control over the different networks which play a role in the power plant control and management processes. The performed vulnerabilities assessment identified 156 major vulnerabilities in the ICS of the target plant. These were classified according to their likelihood of occurrence and potential impact severity. According to this analysis, all main subsystems, and especially the Process Network, the Data Network, and the Process Firewall resulted heavy vulnerable. The Test Centre also includes an observation network, developed with the main purpose of identifying the "anomalous events", which may happen in the system during the experiments, and to store such events in an organized and coherent way, in order to support the security analysis. On the other side, a malware simulator software (MALSIM) has been developed and used to perform security experiments, i.e. to try the injection of viruses, worms or trojan code. The innovation of this component is that it reproduces malware behaviour, allowing at the same time a full control over the experiment, full repeatability and measurability. JRC activities are focused on: • Development and the design of a SCADA simulator; • Analysis of field protocol vulnerabilities; • Implementation of the first proof of concept of a Modbus malware, able to take the control of a power plant field network.
Period	Since 2006
Country	IT
Environment	Energy
URL	http://ipsc.jrc.ec.europa.eu/index.php/epic-description/693/0/

Project name	KEMA Test Centre
Organisation name	DNV KEMA
Brief project description	When developing or buying a system using a standard protocol, it is essential to be sure it complies with the standard. DNV KEMA has facilities for testing IEC protocol implementations. The testing involves a number of elements, including interoperability testing and conformance testing. Interoperability testing entails establishing that data exchange is possible and evaluating application integration

	between systems from different vendors. If systems are able to interoperate, the test result is positive. However, if two systems are able to interoperate, it does not follow that the exchange of data between them must comply with the specifications of the applicable standard. Conformance testing is therefore needed to establish whether a vendor's implementation is compliant. To test compliance, the vendor's system is connected to a reference system maintained by a test organization. Procedures for conformance testing are integral to certain standards (IEC 60870-6, 61850 and DLMS). When testing compliance with these standards, a test organization follows these procedures. DNV KEMA's Protocol Competence and Test Center is the number one test organization for IEC protocols. DNV KEMA was the first independent (level A) test organization authorized by the UCA Users Group to perform the official IEC 61850 conformance tests and issue UCA certificates. In DNV KEMA's experience, more than 90 percent of devices fail the first test. It has been proven that using certified products significantly reduces communication problems when a device enters service. DNV KEMA is well equipped for conformance testing. First it draws up the test plan based on the test procedures and the customer-specific requirements. It uses an advanced conformance test system in combination with a protocol analyzer to test whether a specific device meets the international standard. The test will reveal any interpretation problems and bugs in the software at an early stage (before implementation on the customer's site). Energy companies often require that a product passes a conformance test before they will proceed to purchase. Securing a DNV KEMA or UCA certificate also gives manufacturers a competitive advantage.
Period	Since 2012
Country	NL
Environment	Energy
URL	http://www.dnvkema.com/

Project name	SfP 983805 - SCADA Testbed Simulator: Emergent phenomena testbed simulator for improving SCADA performance in power system security management
Organisation name	Faculty of electrical engineering and computing, University of Zagreb Dipartimento di Elettronica e Informazione, Politecnico di Milano
Brief project description	The project is motivated for new challenges in SCADA development, seeking an improvement in the reliability and safety of the devices that make up ICS environments. They have created a serious simulation platform, comprising both hardware and software. This platform can play all scenarios and analyze the behaviour of each device.

	Among the objectives of the project include the intention to create a Test bed for research, and the integration of commercial products in the Test bed ICS environments. The Test bed performed has as main idea to seek the reliability and security of systems adapted to the smart grid, having a connection to intelligent networks and integrating processes with distributed generation and energy efficiency. The project is comprised of several parts that together form a complete Test bed for trials systems, devices and configurations that can be performed in a Smart Grid system. This achieves collect a very important source of information for subsequent hardening of the devices comprising the infrastructure. The main objectives of the project are: • Studying and assessing the current status of SCADA deployment (with an accent on Italy and Croatia) • Evidentiating similarities and dissimilarities and assessing priorities in future SCADA testbed architecture • Proposing a novel architecture for SCADA component interaction modeling, based on cooperative agent negotiation, to bridge the usefulness of the software-as-a-service model with additional reliability and security • Formally and empirically prove the improvements in security, safety and resilience of this architecture over the ones commonly used • Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardization, accompanied by a raising awareness programme reaching all end-users • Identifying and disseminating best practice, possibly in a joint endeavor between manufacturers and end users, resulting in a joint capability and technology taxonomy of security solutions - Stimulating convergence of current standardization efforts. Liaising with international efforts and especially with the US Process Control Forum • - Development and deployment of SCADA testbed platform for analysis of emergent phenomena in power systems.
Period	Since 2012
Country	HR
Environment	Generic
URL	http://www.fer.unizg.hr/NATO_SNG/

Project name	SCADALAB
Organisation name	INTECO

Brief project description	SCADALAB (SCADA LABoratory and test bed for critical infrastructure protection) is a cyber-security project, funded by EC DG Home, which aims to increase CIP (Critical Infrastructure Protection) capabilities at a European level. This goal will be pursued by developing a living SCADA (Supervisory Control And Data Acquisition) laboratory where to carry out security tests and to experiment new technologies that could prevent, detect and mitigate the effects of cyber attacks in EU member states. The aim of the project is to solve specific problems of current insufficient security measures taken to protect industrial control systems with two main objectives: • Development of a laboratory for security testing utilized by CI security responsibles in order to maintain the EU security environment of critical infrastructures. • Reuse existing assets, knowledge and equipment in an efficient manner with concrete and realistic benefits to achieve by the end of the project: • Definition of security requirements for industrial control systems and a concrete methodology for security testing. • Development of a security laboratory close to the real environment and tested. • Creation of a tool to facilitate efficient testing channels and remote testbed as a service. • Creation of a tool for effective ways of sharing results and experiences. • Smart online and offline dissemination of results for beneficiaries in public and private sectors in the EU. ScadaLab Project focuses on increasing critical infrastructure protection capacity in the transport, energy, ICT, chemical, financial, water, food, health, and space, research and nuclear sectors by developing a living SCADA LAB to test exercises and research SCADA technologies that prevent, detect and mitigate cyber attacks in EU member states. It exists five starting points in the project: 1. ICS Bse architecture 2. Test bed and laboratory area requirements 3. Analysis of existing methodologies 4. Type of security assessment 5. Approach of test inventory SCADA LAB project activities will increase the logical protection capacity, firstly in the energy sector as an initial user case, and then extending the solution to other sector scenarios and beneficiaries. Activities go from identifying potential threats for industrial

	frameworks cyber-security, defining a methodology for testing, buil¬ding a testbed infrastructure, allowing remote testing and sharing results with target groups. Likewise an improvement in protection levels and awareness are expected, putting together public and private organizations from different countries to improve communication. The testing methodology has three phases with differents activities: 1. Planning: • Organizational level • Operational level • Technical level 2. Assessment: - Set the lab - Execution 3. Reporting: - Calculation of the metrics - Report of findings
Period	2012-2014
Country	ES
Environment	Generic
URL	http://jmi.ac.in/upload/fet/SCADA/scada_lab.htm

References

1. **Idaho National Laboratory.** *Wireless Procurement Language in Support of Advanced Metering Infrastructure Security.* 2009.

2. **National Institute of Standards and Technology (NIST).** *NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security.* 2011.

3. **National Institute of Standards and Technology, U.S. Department of Commerce (NIST).** *Recommended Security Controls for Federal Information Systems and Organizations.* 2009.

4. **National Institute of Standards and Technology (NIST).** *Field Device Protection Profile For SCADA Systems In Medium Robustness Environments. .* 2006.

5. —. *System Protection Profile-Industrial Control Systems.* 2004.

6. **Smart Grid Interoperability Panel (SGIP).** *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. The Smart Grid Interoperability Panel Cyber Security Working Group.* 2010.

7. **National Institute of Standards and Technology (NIST).** *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0. Retrieved 2012 from http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf.* 2009.

8. **Smart Grid Interoperability Panel (SGIP).** *Smart Grid Testing & Certification committee (SGTCC) – Status and Overview.* 2011.

9. **Information Trust Institute.** *Deft Cyber-Physical Experimentation Framework. .*

10. —. *EVALUATION TESTBED DEVELOPMENT.*

11. —. *ILLINOIS CENTER FOR A SMARTER ELECTRIC GRID.*

12. **Public Safety Canada.** *Canadian Cyber Incident Response Centre (CCIR).*

13. **Mississippi State University and Washington State University.** *A Control System Test Bed to Validate.*

14. **TCIPG Trustworthy Cyber Infrastructure for the power grid.** *About TCIPG: Trustworthy Cyber Infrastructure for the Power Grid.*

15. **Team for Research in Ubiquitos Secure Technology.** *TRUST for SCADA: A simulation-based Experimental Platform.*

16. **European Commission.** *ERNCIP, European Reference Network for Critical Infrastructure Protection.*

17. **European Network of Secure Test Centres for Reliable ICT-controlled Critical Energy Infrastructures (ESTEC) .** *Final Report.* 2009.

18. **European Network and Informations Security Agency (ENISA).** *Protecting Industrial Control Systems - Recommendations for Europe and Member States.* 2011.

19. **United States General Accounting Office (GAO).** *GAO-04-354: Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* 2004.

20. **Industrial Control Systems Joint Working Group (ICSJWG).** *Common Industrial Control System Vulnerability Disclosure Framework.* 2012.

21. **Idaho National Laboratory (INL).** Idaho National Laboratory. [En línea] https://inlportal.inl.gov/portal/server.pt/community/home.

22. —. National Supervisory Control and Data Acquisition Test Bed. [En línea] http://www.inl.gov/research/national-supervisory-control-and-data-acquisition-test-bed/.

23. **Energetics Incorporated.** *Roadmap to Secure Control Systems in the Energy Sector.* 2006.

24. **Energy.gov.** Office of Electricity Delivery and Energy Reliability. [En línea] http://energy.gov/oe/office-electricity-delivery-and-energy-reliability.

25. —. National SCADA Test Bed. [En línea] http://energy.gov/oe/national-scada-test-bed.

26. **European Network for Cyber Security (ENCS).** The European Network for Cyber Security. [En línea] https://www.encs.eu/.

27. **ISA99.** ISA99 Committee. [En línea] http://isa99.isa.org/ISA99%20Wiki/Home.aspx.

28. **National SCADA Test Bed (NSTB).** *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program.* 2008.

29. **PANLAB Consortium.** *PII - Deliverable 3.2: Testbed Service Description Specification.* 2009.

30. **Sandia National Laboratories (SNL).** National Supervisory Control and Data Acquisition (SCADA). [En línea] 2012. http://energy.sandia.gov/?page_id=859.

31. **SfP 983805 SCADA Testbed Simulator Consortium.** *Emergent Phenomena Testbed Simulator for Improving SCADA Performance in Power System Security Management.* 2013.

32. **Technical Division Industrial Information Technology.** *VDI/VDE 2182 Part 1: IT-security for industrial automation - General model.* 2011.

33. —. *VDI/VDE 2182 Part 3.1: IT-security for industrial automation - Example of use of the general model for manufacturers in factory automation - Process control system of a LDPE plant.* 2011.

34. —. *VDI/VDE 2182 Part 2.1:IT-security for industrial automation - Example of use of the general model for device manufacturer in factory automation - Programmable logic controller (PLC).* 2013.

35. —. *VDI/VDE 2182 Part 2.2: IT-security for industrial automation - Example of use of the general model in factory automation for plant and machinery installers - Forming press.* 2013.

36. —. *VDI/VDE 2182 Part 3.2: IT-security for industrial automation - Example of use of the general model for integrators in process industry - LDPE reactor.* 2013.

37. **The university of Arizona.** Autonomic Critical Infrastructure Protection (ACIP). [En línea] 2011. http://acl.ece.arizona.edu/projects/current/HSSS/.

38. **Viking Project.** Viking Project. [En línea] 2011. http://www.vikingproject.eu.

39. **National Security Agency.** *A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS).* 2010.

40. **International Organization for Standardization (ISO), International Electrotechnical Commission (IEC).** *Information technology — Security techniques — Code of practice for information security management.* International Organization for Standardization, International Electrotechnical Commission. 2005.

41. **National Institute of Standards and Technology (NIST).** *NIST SP 800-53: Information Security.* National Institute of Standards and Technology. 2009.

42. **International Instruments Users' Association (WIB).** *Process control domain - Security requirements for vendors.* EWE (EI, WIB, EXERA). 2010.

43. **International Electrotechnical Commission (IEC).** *IEC 61850-7-2: Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI).* International Electrotechnical Commission. 2010.

44. —. *IEC 61850: Communication networks and systems in substations.* 2011.

45. **CIGRÉ.** *The Impact of Implementing Cyber Security Requirements using IEC 61850.* s.l. : CIGRE Publication 427, 2010.

46. **Defence Science Technology Organisation (DSTO).** *Def(Aust) 5679 "The Procurement Of Computer-based Safety Critical Systems".* s.l. : Land Engineering Agency, 1998.

47. **National Institute of Standards and Technology (NIST).** FIPS PUB 199. *Standards for Security Categorization of Federal Information and Information Systems.* [En línea] 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

48. **US Goverment.** *Federal Information Processing Standard, Security Requirements for Cryptographic Modules .* 2003.

49. **International Standar Orgaitation.** *Conformity assessment - Requirements for bodies certifying products, processes and services (ISO/IEC 17065:2012).* 2012.

50. **7th Framework Programme.** The VIKING projects – Towards more secure SCADA Systems. [En línea] 2012.

51. **ABB Network Management.** *The VIKING Project – Towards more Secure SCADA Systems.*

52. **American Gas Association (AGA).** *Cryptographic Protection of SCADA Communications. Part 1: Background, Policies and Test Plan (AGA 12, Part 1).* 2006.

53. **British Columbia Institute of Technology (BCIT).** *Industrial Instrumentation Process Lab.*

54. **Critical Utility Infrastructural relisence.** *WP3 Testbed development.*

55. **Deutsches Institut für Normung e. V. (DIN). .** *DIN.*

56. **Digital Bond.** *Why Crain / Sistrunk Vulns Are A Big Deal.* 2013.

57. **ENEA .** *FINAL REPORT Feasibility Study: European Network of Secure Test Centres for Reliable ICT-controlled Critical Energy Infrastructures (ESTEC).* 2007.

58. **Office of Electricity Delivery & Energy Reliability.** *NATIONAL SCADA TEST BED.* 2003.

59. **European Commision.** *European Commission.*

60. **European Commission.** *ISA: a programme for targeted action.*

61. **European SCADA and Control Systems Information Exchange (EuroSCSIE).** *Welcome to the EuroSCSIE Workspace.*

62. **Global Cyber Security Center (GCSEC).** *The European SCADA and Control System Information Exchange.*

63. **Homeland Security.** *DETER-Enabled Federated Testbeds (DEFT).*

64. **Idaho National Laboratory (INL).** *Project Completion Report, Critical Infrastructure Test Range Program at Idaho National Laboratory.* 2005.

65. **Information Trust Institute.** *ABOUT US.*

66. **Institut für Automatik – Automatic Control Laboratory.** *VIKING Project.*

67. **International Instruments Users' Association (WIB).** *Process control domain - Security requirements for vendors. EWE (EI, WIB, EXERA).* 2010.

68. **International Society of Automation (ISA).** *ISA99, Industrial Automation and Control Systems Security.*

69. **ISA Secure.** *ISASecure Program Description.*

70. **ISA99 Committee.** *ISA99 Committee on Industrial Automation and Control Systems Security.*

71. **Jeju Smart Grid Test-Bed.** *Jeju Smart Grid Test-Bed.*

72. **KTH ROYAL INSTITUTE OF TECHNOLOGY.** *VIKING.* 2013.

73. **National Institute of Standards and Technology (NIST).** *NIST Smart Grid Collaboration Wiki for Smart Grid Interoperability Standards.*

74. **National Institute of Standards and Technology.** *Interagency Grantees Meeting/Workshop Nanotechnology and the Environment: Applications and Implications.*

75. **Oak Ridge National Laboratory.** *A Physical Protection Systems Test Bed for International Counter-Trafficking System Development.*

76. **Sandia LabNews, Sandia National Laboratories.** *DOE standards group to fast-track energy security improvements in US critical infrastructure systems.* 2004.

77. **Sandia Natioanl Laboratories.** *Virtual Control System Environment.*

78. **Sandia National Laboratories.** *FY 2013 Twenty-Five-Year Site Plan.* 2012.

79. —. *Sandia National Labs. Exceptional service in the nation interest.*

80. **SciTech Connect.** *A Physical Protection Systems Test Bed for International Counter-Trafficking System Development.* 2011.

81. **Security dark Readin.** *SCADA 'Sandbox' Tests Real-World Impact Of Cyberattacks On Critical Infrastructure.* 2013.

82. **Southeast Region Research Initiative (SERRI).** *Southeast Region Research Initiative: MRI (Mississippi Research Initiative).*

83. **TCIPG Trustworthy Cyber Infrastructure for the power grid.** *Testbed Overview.*

84. **The Deter Project.** *EMIST Project Overview.* 2004.

85. **The DETER Project.** *DeterLab: Accelerating Cyber-Security Advances.*

86. —. *EMIST Project Overview.*

87. **The European Network for Cyber Security (ENCS).** *The European Network for Cyber Security (ENCS).*

88. **U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability.** *CERTS Microgrid Test Bed. Phase III Activities. Role of Microgrids in Facilitating Integration of Distributed Renewable Electricity Sources.* 2009.

89. **UCA.** *UCA International Users Group from http://www.ucaiug.org/default.aspx.*

90. **University of Illinois at Urbana-Champaign.** *The Virtual Power System Testbed and Inter-Testbed Integration.*

91. **USC Information Sciences Institute.** *A Federated Experiment Environment for Emulab-based Testbeds.*

TP-02-13-769-EN-

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-074
9 789292 04074
doi: 10.2824/26451

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu