# CYBER SECURITY OF SAFETY-CRITICAL INFRASTRUCTURES: A CASE STUDY FOR NUCLEAR FACILITIES

Vladimir SKLYAR

**Abstract:** Computers have become crucial to the operations of government and business. Critical infrastructure protection policy has evolved since the mid-1990's. Since 11 September 2001, the critical link between cyberspace and physical space has been increasingly recognized. Presently, critical infrastructure sectors face various cyber threats. In particular, the electrical power infrastructure is the most critical infrastructure upon which other infrastructures depend. Cyber attacks on energy production and distribution systems could endanger public health and safety, damage the environment, and have serious financial implications, such as loss of production, generation, or distribution of public utilities; compromise proprietary information; or bring liability issues.[1] Government and private sector computer security is affected by various laws, but not all laws reflect newly emerging challenges. At the same, time poor systems management can be costly and disruptive. This paper presents an approach allowing to implement, manage and maintain cyber security program for Instrumentation and Control (I&C) systems of Nuclear Power plants (NPP). It is based on existing standards' requirements consideration of issues specific to the security of Field Programmable Gates Arrays (FPGA).

**Keywords:** Critical Infrastructure, complexity, vulnerability, nuclear power plant, NPP, information security standards, Stuxnet.

## Introduction

Usually nation's critical infrastructures include those assets, systems, and functions vital to our national security, economic need, or national public health and safety. Critical infrastructures encompass a number of sectors, including many basic necessities of our daily lives, such as food, water, public health, emergency services, energy, transportation, information technology and telecommunications, banking and finance, and postal services and shipping. All of these critical infrastructures increasingly rely on computers and networks for their operations.[2]

The objective of cyber security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to

remain accessible and productive to its intended users.[3] Presently cyber security issues are the most important challenge of Information Technologies (IT) development. Global infrastructures dependency from IT increases with IT complexity and vulnerability increasing. Transport, power engineering, government affaires management, military area and other critical infrastructures are becoming an object of malicious cyber attacks. For example, the following US critical infrastructure sectors needed to be protected against cyber-attacks (see Table 1).

Profile of infrastructure-specific cyber security requirements has to be selected on the basis of assets and threats analysis. In particular, the electric power infrastructure is the most critical infrastructure upon which other infrastructures depend. Threats to the power infrastructure include natural disasters, human errors, power system component failures, information and communication system failures, gaming in the electricity markets, intrusion, and sabotage. Strategic Power Infrastructure Defence (SPID) system methodology has been suggested as a real-time, wide-area, adaptive protection and control system involving the power, communication, and computer infrastructures.[4] The proposed The SPID system performs the failure analysis, vulnerability assessment, and adaptive control actions to avoid catastrophic power outages.

The goal of this paper is to observe an approach to cyber security implementation for NPP I&C systems as well as to propose an approach to cyber security improvement on the basis of FPGA technology.

## Common Cyber Security Technologies

There are a number of cyber security technologies that can be used to better protect critical infrastructures from cyber attacks. In each of these categories, many technologies are currently available, while other technologies are still being researched and developed. Table 2 summarizes some of the common cyber security technologies, categorized by the type of security control they help to implement. Critical infrastructure sectors use all of these types of cyber security technologies to protect their systems. However, the level of use of technologies varies across sectors and across entities within sectors.

There are a lot of different approaches to implement and manage cyber security measures. On from the approaches is Open Security Architecture (OSA). The OSA Metamodel depicts the entities and relationships that are relevant for OSA (see Figure 1). OSA can provide benefits to IT service consumers, IT service suppliers and IT vendors, giving the entire IT community an interest in using and improving. An open approach means that the patterns and catalogues will benefit the whole community and can be more quickly improved and refined by the common experience of participants.

Table 1. Critical Infrastructure Sectors Defined in USA Federal Critical Infrastructure Protection Policy.

| ***Sector*** | ***Description*** |
|---|---|
| Agriculture | Includes supply chains for feed and crop production |
| Banking and finance | Consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement |
| Chemicals and hazardous materials | Produces products essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities |
| Defence industrial base | Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance |
| Emergency services | Includes fire, rescue, emergency medical services, and law enforcement organizations |
| Energy | Includes electric power and the refining, storage, and distribution of oil and natural gas |
| Food | Covers the infrastructures involved in post-harvest handling of the food supply, including processing and retail sales |
| Government | Ensures national security and freedom and administers key public functions |
| Information technology and telecommunications | Provides information processing systems, processes, and communications systems to meet the needs of businesses and government |
| Postal and shipping | Includes the Postal Service and other carriers that deliver private and commercial letters, packages, and bulk assets |
| Public health and healthcare | Consists of health departments, clinics, and hospitals |
| Transportation | Includes aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit that are vital to economy, mobility, and security |
| Drinking water and water treatment systems | Includes public water systems that rely on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines |

Table 2. Cyber Security Technology Control Categories and Types.

| *Control category* | *Control type* |
|---|---|
| Access controls | Boundary protection: Firewalls, Content management |
| | Authentication: Biometrics, Smart tokens |
| | Authorization: User rights and privileges |
| System integrity | Antivirus software |
| | File integrity checkers |
| Cryptography | Digital signatures and certificates |
| | Virtual private networks |
| Audit and monitoring | Intrusion detection systems |
| | Intrusion prevention systems |
| | Security event correlation tools |
| | Computer forensics tools |
| Configuration management and assurance | Policy enforcement applications |
| | Network management |
| | Continuity of operations |
| | Scanners |
| | Patch management |

## Stuxnet-worm case study

I&C systems and other forms of networked computer systems have been used for years to control power grids and units. These systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions as well as to enhance performance. It has created a lot of vulnerabilities for safety critical control systems. A recent incident with Stuxnet-worm discovered a new type of cyber attack by malicious software in compromised Programmable Logic Controllers (PLC).

The discovery in June 2010 of the Stuxnet worm and subsequent reverse engineering and analysis of the worm by computer security experts has revealed that Stuxnet was primarily written for espionage and sabotage of a specific instance of industrial control systems used in an enrichment plant. Its final goal is to spy on the targeted industrial systems and reprogram industrial control systems by modifying code on PLCs to make them work in a manner the attacker intends and to hide those changes from the operator of the equipment.[5]

Stuxnet's goal is to modify the behavior of an industrial control system by modifying PLCs. It does this by intercepting read/write requests sent to the PLC, determining whether the system is the intended target, modifying the existing PLC code blocks and writing new blocks to the PLC, and finally hiding the PLC infection from the PLC operator/programmer using rootkit functionality. The tasks are distinct because, for instance, the hiding of infected code blocks takes place on the infected Windows machine using standard C/C++ code whereas the malicious code that Stuxnet aims to run on the industrial control system execute on the PLC and are written in MC7 byte-code. MC7 is the assembly language that runs on PLCs (Figure 2).[6]

Stuxnet is of such great complexity that few attackers will be capable of producing a similar threat. However, Stuxnet has highlighted the fact that direct-attack attempts on critical infrastructure are possible and not just theory or movie plotlines. The real-world implications of Stuxnet are beyond any threat seen in the past. Some are calling Stuxnet the "first weapons grade computer virus." Stuxnet can also present a serious threat to operating NPPs because some plants are operated with such type of PLCs which were attacked.

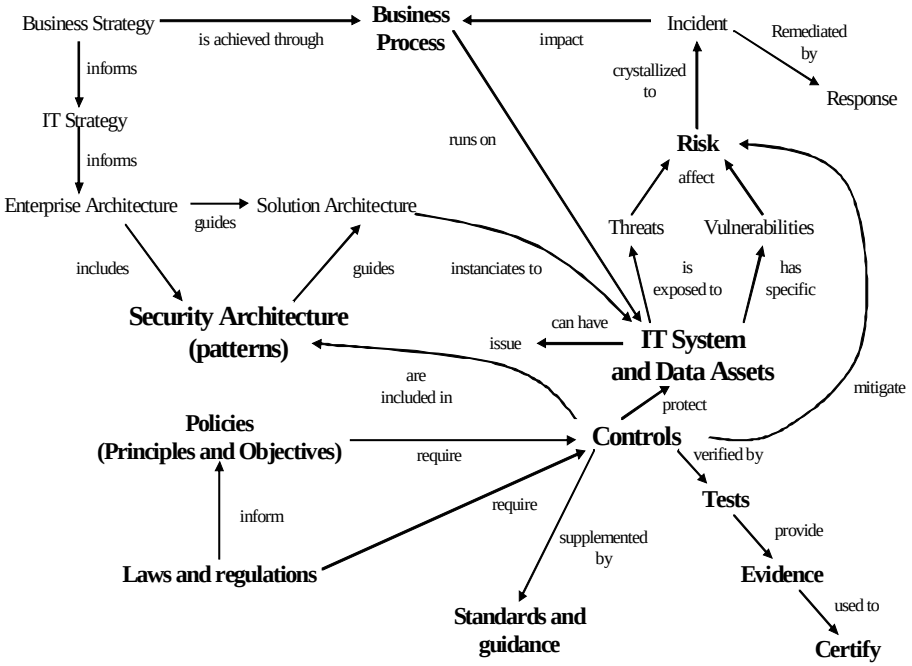


Figure 1. Open Security Architecture (OSA) Metamodel

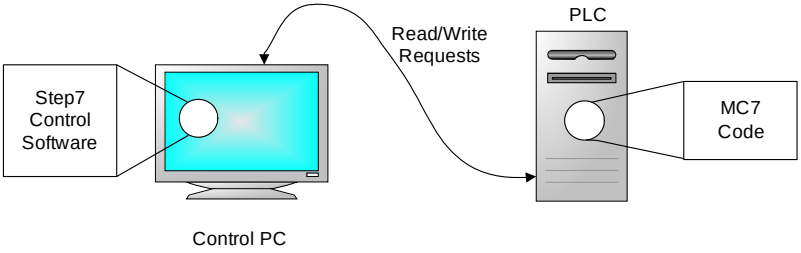


Figure 2. A way to insert Stuxnet PLC-based control system.

## Analysis of requirements to cyber security of NPP I&C systems

Requirements to cyber security of NPP I&C systems are mainly extracted from the general IT security requirements, such as ISO/IEC 27000 standards series. This set of standards includes the following (some another parts now have been developed):

- ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary;
- ISO/IEC 27001:2005 Information technology - Information security management systems - Requirements;
- ISO/IEC 27002:2005 Information technology - Code of practice for information security management;
- ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management;
- ISO/IEC 27006:2007 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.

The most mature requirements to cyber security of NPP I&C systems are developed by US Nuclear Regulatory Commission which is Nuclear Regulatory Authority. The last such guide US NRC 5.71 “Cyber Security Programs For Nuclear Facilities” was developed in 2010.[7] The supporting document NEI 08-09 was developed by the U.S. Nuclear Energy Institute.[8]

International Electrotechnical Commission (IEC) and International Atomic Energy Agency (IAEA) also develop standards related to I&C systems cyber security:

- IEC 62645 CD1 Nuclear Power Plants – Instrumentation and control important to safety – Requirements for security programmes for digital I&C systems (2010);
- IAEA Nuclear Security Series, Draft Reference Manual, Computer Security at Nuclear Facilities (2011);

- Different standards use different approaches to cyber security implementation and management and even different basic terms and definition. Table 3 presents comparative analysis results for the main entity of such standards as IAEA Computer Security Draft, US NRC RG 5.71 and IEC 62645 Draft.

Cyber Security life cycle includes activities for each of the stage of system development and operation such as: Planning Phase, Requirements Phase, Design Phase, Implementation Phase, Validation Phase, Installation and Acceptance Testing Phase, Operations and Maintenance Phase, Change Management, Retirement Phase.

## An approach to improving cyber security based on FPGA technology

FPGA is a semiconductor device that can be programmed after manufacturing. Features and functions of this hardware are programmed by hardware description language (HDL) or by schematic drawing in Integrated Design Environments (IDE).[9]

FPGA-based technologies also have specific beneficial properties regarding security that are different from those of PLC-based technologies such as:

- HDL code (usually VHDL or Verilog) without an operating system is used for FPGA programming. At the present there are no known viruses and malware for HDL;
- FPGA-based designs do not rely on an operating system and therefore do not have dormant, unused capabilities that can be attacked;
- Some PLD are not reprogrammable (like ASIC) and program modification requires the physical replacement of the ASIC-based board;
- Some PLD (like CPLD and FPGA) are reprogrammable. HDL code is located in flash memory (separated chip) without physical access for modification;
- FPGA programming and reprogramming can be done only through a special interface. It is impossible to connect common storage media or communication devices that could infect the control logic code, as was the case with the Stuxnet;
- FPGA-based devices have simpler designs (compared to conventional PLC-based solutions). It entails more likely possibilities to detect malicious designs by V&V. It also permits to assess COTS-based design;
- Each FPGA design has a higher degree of uniqueness compared to software-based designs. For example each circuit family is different from the others and require specific development tools. So it is impossible to develop a common malware which would be appropriate to infect many types of FPGA-based systems with different PLD.

Table 3. Comparative analysis of the main requirements of IAEA draft, US NRC RG 5.71 and IEC 62645 CD1

| *Document categories* | *IAEA draft (66 pages)* | *US NRC RG 5.71 (105 pp.)* | *IEC 62645 CD1 (37 pages)* |
|---|---|---|---|
| Main entity and definition | Computer security (synonym of cyber security) is a particular aspect of information security related to computer based systems, networks and digital systems.<br>Information security - the security of any information regardless of the media used to store or transmit the information. Includes the preservation of the confidentiality, integrity and availability attributes of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.<br>Personnel security, Physical security, Nuclear security (in 1.2.1, not in Glossary) | There is no security definitions<br>Cyber security - protection against cyber attacks is meant | No security definitions<br>Computer security - reference to IAEA guidance<br>The goal of the computer-based security is to protect the I&C systems from deliberate and intelligent attacks that may jeopardise overall plant safety and availability. |
| Security control | Management systems, Organizational issues, Implementing computer security | Technical, Operational and Management control | 11 security categories and Security Programme management |
| Related documents | Site Security Plan<br>Computer Security Plan (can be a part of SSP) | Cyber Security Plan<br>Cyber Security Program | Security Programme<br>Computer Security Plan |
| Requirements to vendors | It is paramount that the security department works closely with the contracts department to ensure that the security provisions are incorporated in each contract.<br>When considered necessary, checks and audits should be made to ensure that the contracting organization's management system adequately addresses security issues, and that the organization's practices and measures are in compliance with the system. | There are no direct requirements, only from utility point of view | There are no direct requirements.<br>Platform and application security is a part of operational security procedures |
| Life cycle | Security management lifecycle (spiral shape) | Security lifecycle process (spiral shape) | Linear Life Cycle Implementation of Computer Security |
| Levels of security | Five levels of security (strength of measures) | Five levels of cyber security defensive architecture | Five levels of computer security protective measures |

Considering of possible scenarios to insert malware in HDL code can discover strengths and weaknesses of FPGA-based technologies. Results of scenarios demon-

strated that at the present risk of FLGA-based devices infection is much more less then for PLCs. The main such scenarios can be as the following:

Scenario 1. *Internal threats*: Malware can be inserted in HDL code by malicious developer during design or modification. Risk can be prevented by independent V&V under strong design and modification procedures. It is possible to find supernormal code and functions by code inspections and testing.

Scenario 2.1. *External threats*: Malware can be inserted in HDL code by malicious tools (IDE – Integrated Design Environment). There is no viruses and malware for IDE, but it can appear in the future. Risk can be prevented by tools assessment.

Scenario 2.2. *External threats*: Malware can be inserted in HDL code by compromised programming device. Risk can be prevented by cyber security measures for programming device.

## Conclusions

Currently, the importance of cyber security importance for safety-critical infrastructures is raising quickly. An approach to improve cyber security can include procedures such as:

- Harmonization of terminology and requirements;
- Establishing Cyber Security policy and programmes;
- Incorporating the cyber security programme into the programme for physical protection;
- Using programmable components with smaller degree of vulnerability (Programmable Logic Devices versus PLC);
- Access control for development and programming tools;
- Using tools for V&V which are different from development tools;
- Participation in appropriate conferences and standards development;
- Analysis of threats and cyber attack scenarios. Threat analysis has to consider possibilities to develop malware for different types of controllers, infect different types of controllers (PLC, ASIC, PLD, FPGA, microCPU), detect malware in controllers, possible features of malware.

Best cyber security practices which can be recommended to community as a part of protection policy of NPP I&C systems include the following:

- Programming device disconnection from safety (non-safety) controllers during operation provides really security improvement versus Engineering Workstations continuously connected with I&C system;
- Media for controllers programming should be forbidden;

- Authentication should be implemented for access to controllers' code;
- Ports for controllers programming should be not widely used (for example, JTAG versus 8P8C [RJ45]);
- Fast encryption algorithms should be used for external communications as well as for data archives. It does not decrease systems availability;
- On-line Data Base should be available for events archiving and analysis;
- Rooms and spaces for communication cables should be locked and access procedures should be implemented;
- Permanent monitoring of hardware and software security data during operation has been implemented.

## Notes:

[1] United States General Accounting Office (GAO), *Technology Assessment. Cybersecurity for Critical Infrastructure Protection*, GAO-04-321 (Washington, D.C.: GAO, 2004); *Cyber Space Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: The White House, 2010).

[2] Ibid.

[3] National Institute of Standards and Technology (NIST), *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53. Revision 3, 2009.

[4] Hao Li, Gary W. Rosenwald, Juhwan Jung, and Chen-Ching Liu, "Strategic Power Infrastructure Defense," *Proceedings of the IEEE* 93:5 (2005), 918-33.

[5] Albright D., Brannan P., Walrond C., *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (Institute for Science and International Security, 2010).

[6] Nicolas Falliere, "Exploring Stuxnet's PLC Infection Process," *Symantec Connect*, 22 Sep. 2010, <www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process>.

[7] United States Nuclear Regulatory Commission, *Cyber Security Programs For Nuclear Facilities*, Regulatory Guide 5.71, 2010.

[8] *Cyber Security Plan for Nuclear Power Reactors*, NEI 08-09, Rev. 6 (Washington D.C.: Nuclear Energy Institute, 2010)

[9] Vyacheslav Kharchenko and Vladimir Sklyar, eds., *FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment* (Kirovograd: RPC Radiy, 2008).

**VLADIMIR SKLYAR** is Technical Director of Research and Production Corporation Radiy (Ukraine), which is a designer and manufacturer of Instrumentation and Control systems for Nuclear Power Plants, as well as an Associated Professor of the Computer Systems and Networks Department, National Aerospace University "Kharkiv Aviation Institute" (Ukraine). His research interests lay in safety and dependability of safety critical computer systems. He graduated from Kharkiv Military University (Ukraine) in 1992 and received a PhD degree in computer engineering from Kharkiv Military University (Ukraine, 2001).