When Recognition Matters

PECB Certified

Lead SCADA Security Manager

The objective of the "PECB Certified Lead SCADA Security Manager" examination is to ensure that the candidate has the knowledge and skills to support an organization in implementing and managing security programs for the protection of SCADA systems. If you are an executive, senior manager, experienced project manager, consultant and/or ISO auditor wanting to understand the value of SCADA systems in your organization, to certify your skills, to stand out to employers/clients and to maximize your earning potential, then the "PECB Certified Lead SCADA Security Manager" credential is the right choice for you.

The target population for this examination is:

- Security professionals seeking to gain SCADA security skills
- IT staff looking to enhance their technical skills and knowledge
- IT and Risk Managers seeking a more detailed understanding of ICS and SCADA systems
- SCADA system developers
- SCADA Engineers and Operators
- SCADA IT personnel

The exam content covers the following domains:

- Domain 1: Fundamental principles and concepts of SCADA and SCADA Security
- Domain 2: Industrial Control Systems (ICS) characteristics, threats and vulnerabilities
- Domain 3: Designing and Developing an ICS Security Program based on NIST SP 800-82
- Domain 4: Network Security Architecture for SCADA Systems
- Domain 5: Implementation of Security Controls for SCADA Systems
- Domain 6: Developing Resilient and Robust SCADA Systems
- Domain 7: Security testing of SCADA Systems

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of SCADA and SCADA Security

Main objective: To ensure that the Certified Lead SCADA Security Manager candidate can understand, interpret and illustrate the main concepts and principles related to SCADA Systems and associated security concepts.

Competencies	Knowledge statements
1. Understand and explain the purposes of SCADA Systems, Distributed Control Systems and Programmable Logic Controllers. 2. Ability to understand the key operation of ICS systems. 3. Ability to explain and distinguish the differences between ICS control and network components 4. Ability to define the key characteristics of SCADA Systems 5. Ability to define the key characteristics of Distributed Control Systems 6. Ability to define the key characteristics of Programmable Logic Controllers 7. Ability to understand and describe industrial sectors and their interdependencies and the association with security 8. Ability to describe future trends and developments in SCADA Security	1. Knowledge of the different SCADA Systems and their purposes 2. Knowledge of the operations of ICS Systems 3. Knowledge of the main industry standards related to SCADA and SCADA Security 4. Knowledge of the basic working elements of ICS control and network components 5. Knowledge of the differences and characteristics of DCS, PLCs and SCADA Systems 6. Knowledge of how SCADA Systems are interdependent between industries and the relevant security issues. 7. Knowledge of future trends and developments in SCADA Security

Domain 2: Industrial Control Systems (ICS) characteristics, threats and vulnerabilities

Main objective: To ensure that the Certified Lead SCADA Security Manager candidate can understand, the common threats and vulnerabilities related to ICS systems and how they can be managed.

Competencies	Knowledge statements
1. Ability to describe the differences between traditional IT Security risks and ICS Security risks 2. Ability to conduct a threat assessment in order to both identify and prioritize the importance of threats in a given environment 3. Ability to explain policy and procedural vulnerabilities and how these vulnerabilities could lead to a security compromise 4. Ability to explain platform vulnerabilities and how these vulnerabilities could lead to a security compromise 5. Ability to explain network vulnerabilities and how these vulnerabilities could lead to a security compromise 6. Ability to conduct a risk assessment of a SCADA environment and present the findings 7. Ability to understand the common attack vectors against SCADA systems and to be able to describe compromises	1. Knowledge of common ICS security risks 2. Knowledge of techniques for identifying and assessing threats 3. Knowledge of the common threats to SCADA environments 4. Knowledge of the common vulnerabilities in SCADA environments 5. Knowledge of the different types of vulnerabilities faced in SCADA environments 6. Knowledge of risk assessment processes and methodologies used to assess SCADA environments 7. Knowledge of exercising and testing 8. Knowledge of attack vectors which are commonly used against SCADA environments 9. Knowledge of previous incidents and the techniques used along with vulnerabilities exploited

Domain 3: Designing and Developing an ICS Security Program based on NIST SP 800-82

Main objective: To ensure that the Certified Lead SCADA Security Manager candidate can plan, design and implement an effective program to protect SCADA systems.

Competencies	Knowledge statements
1. Ability to develop a clear business case for the development and implementation of a pro-active SCADA security program 2. Ability to obtain and maintain support for the security program from executive management 3. Ability to define and build a suitable cross functional team to support and maintain the security program 4. Ability to develop appropriate policies, procedures, standards and guidelines which are required to support the security program 5. Ability to identify, document and prioritise ICS assets to allow the implementation of an effective security program 6. Ability to establish a pro-active vulnerability management program in the SCADA environment 7. Ability to design and develop security awareness and training materials need in a successful SCADA security program 8. Ability to define measures and metrics to measure the progress of the program	1. Knowledge of the main project management concepts, terminology, process and best practice as described in ISO 10006 2. Knowledge of the principal approaches and methodology frameworks to implement a security program 3. Knowledge of the main concepts and terminology related to organizations 4. Knowledge of an organization's external and internal environment 5. Knowledge of the main interested parties related to an organization and their characteristics 6. Knowledge of techniques to gather information necessary to design the security program 7. Knowledge of the differences between and the purposes of policies, procedures, standards and guidelines 8. Knowledge of vulnerability management techniques and tools and their deployment in a SCADA environment 9. Knowledge of security awareness raising techniques and their application 10. Knowledge of the techniques used to measure the performance of programs and security controls

Domain 4: Network Security Architecture for SCADA Systems

Main objective: To ensure that the Certified Lead SCADA Security Manager has a thorough understanding of network security related to SCADA environments and the techniques used to defend such networks.

Competencies	Knowledge statements
1. Ability to understand firewall technology and its application in a SCADA environment 2. Ability to identify and select the most suitable options for network segregation in a SCADA environment based on the associated risks 3. Ability to define and design a network architecture with suitable defense in depth controls that are proportionate to the risks identified 4. Ability to define clear firewall rulesets based on a strong understanding of key protocols and the security issues that they present 5. Ability to understand and describe SCADA and industrial protocols and the associated security challenges they present 6. Ability identify single point of failure and other design risks in SCADA systems 7. Ability to design resilient SCADA network architectures that are fault tolerant and are designed to address common vulnerabilities and threats	1. Knowledge of firewall technology and its deployment in SCADA environments 2. Knowledge of network design principles and methods for network segregation that can be applied 3. Knowledge of common network protocols including but not limited to DNS, HTTP, FTP, Telnet, SMTP, SNMP and DCOM and the associated security issues 4. Knowledge of SCADA and industrial protocols including how they work and the associated security issues 5. Knowledge of network design principles including resilience and single points of failure 6. Knowledge of remote access technologies and techniques and the associated security vulnerabilities

Domain 5: Implementation of Security Controls for SCADA Systems

Main objective: To ensure that Certified Lead SCADA Security Manager Candidate can understand the possible controls that can be applied to manage SCADA security risks along with the challenges, benefits and issues to be considered

Competencies	Knowledge statements
1. Ability to understand the difference between management, operational and technical controls 2. Ability and explain the relationship between management, operational and technical controls in a SCADA security program 3. Ability to define a process for system and supplier selection based on risk and clear security requirements 4. Ability to design security controls that protect systems and people from a physical security perspective 5. Ability to design controls that deal with operational risks surrounding media protection, information integrity and system availability 6. Ability to understand the options for identity and access management in SCADA environments 7. Ability to understand the options for auditing and log management in SCADA environments	1. Knowledge of the principles of management, operational and technical controls 2. Knowledge of techniques and controls to be used surrounding third party and supplier management 3. Knowledge of common physical security controls used in SCADA environments 4. Knowledge of common personnel security controls used in SCADA environments 5. Knowledge of identity and access management controls that can be applied in a SCADA environment 6. Knowledge of audit and log management techniques and technologies that can be used in SCADA environments

Domain 6: Developing Resilient and Robust SCADA Systems

Main objective: To ensure that the Certified SCADA Security Manager has a complete understanding of how SCADA systems should be resilient and recoverable in the event of an incident or major business interruption

Competencies	Knowledge statements
1. Ability to identify failure points in SCADA system builds, designs and architectures 2. Ability to design resilient high availability SCADA systems 3. Ability to design and execute testing of resiliency controls 4. Ability to define the differences and linkages between security incident management, business continuity and disaster recovery 5. Ability to develop a clear security incident response process based on industry standards such as ISO 27035 6. Ability to develop disaster recovery plans for SCADA systems and facilities that align to the requirements of the business continuity plan 7. Ability to organise and execute testing strategies and processes to ensure that the incident response, business continuity and disaster recovery processes are fit for purpose for use in a real world incident/event 8. Ability to analyse results of such testing activities	1. Knowledge of failure points in SCADA systems, design and architectures 2. Knowledge of the controls and solutions available to aid system resilience 3. Knowledge of techniques that can be used to test resilience controls 4. Knowledge of the differences and linkages between security incident management, business continuity and disaster recovery 5. Knowledge of the disaster recovery planning process and the fundamental elements of a disaster recovery plan 6. Knowledge of the relationship between business continuity and disaster recovery 7. Knowledge of testing strategies for business continuity, disaster recovery and incident management and how to perform such tests

Domain 7: Security testing of SCADA Systems

Main objective: To ensure that the Certified Lead SCADA Security Manager candidate can organise and lead an effective program of security testing for key SCADA systems.

Competencies	Knowledge statements
1. Ability to manage a project to of security testing activities 2. Ability to gather, analyze and interpret the necessary information to scope and plan the testing activities 3. Ability to state and justify a testing scope, and approach based on the risks faced by the organisation. 4. Ability to select and justify the selected approach and methodology adapted to the needs of the organization. 5. Ability to develop a plan taking into account the best practices and associated risks related to the tests. 6. Ability to review results of tests and formulate these into findings 7. Ability to analyze the risk level and present findings in a logical risk based order 8. Ability to group findings in a logical manner 9. Ability to make clear understandable recommendations 10. Ability to develop reports in a business language which express risk and can link into an organisations risk management process 11. Ability to present findings and recommendations to both technical and non-technical audiences	1. Knowledge of the principal approaches and methodology frameworks to implement a testing framework 2. Knowledge of an organization's external and internal environment 3. Knowledge of techniques to gather information necessary to develop a scope and plan. 4. Knowledge of the characteristics of a security testing scope. 5. Knowledge of analysis techniques to analyze information which has been collected 6. Knowledge of risk management and how to analyze the associated risk level of a finding 7. Knowledge of reporting techniques and styles 8. Knowledge of communication techniques

Based on these 7 domains and their relevance, 115 questions are included in the exam. The passing score is established at **60% (69/115).**

			Level of Understanding (Cognitive/Taxonomy) Required					
		Points per Question	Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points per competency domain
Competency/Domains	Fundamental principles and concepts of SCADA and SCADA Security	1	X		16	13.91	16	13.91
	Industrial Control Systems (ICS) characteristics, threats and vulnerabilities	1	X		16	13.91	16	13.91
	Designing and Developing an ICS Security Program based on NIST SP 800-82	1		X	17	14.78	17	14.78
	Network Security Architecture for SCADA Systems	1		X	17	14.78	17	14.78
	Implementation of Security Controls for SCADA Systems	1		X	17	14.78	17	14.78
	Developing Resilient and Robust Systems	1	X		16	13.91	16	13.91
	Security testing of SCADA Systems	1	X		16	13.91	16	13.91
Total points		115						
Number of Questions per level of understanding			64	51				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			55.65	44.35				

After successfully passing the exam, the candidates will be able to apply for the credentials of PECB Certified Lead SCADA Security Manager, depending on their level of experience.

TAKE THE CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the proctor and the exam confirmation letter.

The exam duration is three (3) hours.

The questions are multiple choice questions. This type of format was chosen because it measures different levels of studying, and has resulted to be an effective assessment tool. The multiple-choice exam can be used to evaluate a candidate's understanding on many subjects, including both simple and complicated concepts. First and foremost, multiple-choice exam will not commonly demonstrate if the candidate's response is right or wrong, additionally it will demonstrate continuance of the learning process. Because of this particularity, the exam is not "open book" and does not measure the recall of data or information. This type of examination can be adapted to the measurement of a wide range of learning objectives including: reasoning, problem solving, exercising judgement, making inferences and demonstrating knowledge of facts through analysis and interpretation of information. At the end of this document, you will find sample exam questions and their possible answers.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limitation on how many times a candidate can retake the same exam. However, there are some limitations in terms of allowed time-frame in between exams.

When candidates fail the examination, they are only allowed to retake the examination once within 12 months after the first attempt. If second examination is unsuccessful, candidates will be allowed to retake the exam only after 1 year (12 months). Retake fee applies.

Only candidates, who have completed a full PECB training but fail the written exam, are eligible to retake the exam for free, under one condition:

“A candidate can only retake the exam once and this retake must occur within 12 months from the initial exam’s date.”

When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate’s application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS

1. **The main reason for developing a comprehensive business case when proposing an ICS Security Programme is to:**
   a. Encourage all members of the organisation to support security and to contribute to improving security
   b. Secure funding for the necessary security tools, products and software to protect the SCADA/ICS environment
   c. Provide management with the information needed to make decisions about how the organisation will approach security going forward

2. **You are conducting a risk assessment of a HMI application and have identified that the web interface could be subject to a Cross Site Request Forgery attack from a hacker. What have you identified?**
   a. Vulnerability
   b. Threat
   c. Impact

3. **Some organisations segregate their ICS/SCADA networks from corporate networks using dual homed network cards. Why does this practice pose a potential security risk?**
   a. Because of the network card develops a fault neither network can be accessed.
   b. Because there is generally no filtering in place so essentially the two networks are connected together
   c. Because the network card could become overloaded with traffic causing outages

4. **When using a DMZ network architecture to segregate corporate and SCADA/ICS what would be the advantage of having differing patch management solutions in both environments?**
   a. Patching regimes for ICS/SCADA systems are different from those in corporate IT as patches may cause system downtime or outages and need to be carefully controlled.
   b. Due to the criticality of ICS/SCADA systems patches must be rolled out immediately in these environments and specific solution is therefore required.
   c. ICS/SCADA systems do not use the same software and hardware as corporate IT environments and therefore the corporate IT patch solution is not appropriate.

5. **When considering Domain Name Service (DNS) which of the following is known security vulnerability?**
   a. Session hi-jacking
   b. Brute forcing
   c. Cache poisoning

6. **What does the abbreviation DCS stand for in an Industrial control system context?**
   a. Distributed Computer System (DCS)
   b. Distributed Communication System (DCS)
   c. Distributed Control System (DCS)

7. The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and desktop environments should be addressed:

a. In an informal agreement between the two organisations

b. In a contract agreed between the parties

c. Verbally in a meeting