PECB BEYOND RECOGNITION

Candidate Handbook

PECB Certified Lead SCADA Security Manager

GENERAL

The objective of the “PECB Certified Lead SCADA Security Manager” examination is to ensure that the candidate has acquired the necessary expertise 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 SCADA Lead Security Manager exam is intended for:

- 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 the 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: Ensure that the Certified Lead SCADA Security Manager candidate understands, is able to interpret and illustrate the main concepts and principles related to SCADA Systems and associated security concepts

Competencies	Knowledge statements
1. Ability to 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:** Ensure that the Certified Lead SCADA Security Manager candidate understands 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: Ensure that the Certified Lead SCADA Security Manager candidate is able to plan, design and implement an effective program to protect SCADA systems

Competencies

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

Knowledge statements

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: 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: Ensure that Certified Lead SCADA Security Manager Candidate understands 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: 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: Ensure that the Certified Lead SCADA Security Manager candidate is able to 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, 150 questions are included in the exam. The passing score is established at **70% (105/150).**

			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		27	18	27	18
	Industrial Control Systems (ICS) characteristics, threats and vulnerabilities	1	X		35	23.33	35	23.33
	Designing and Developing the ICS Security Program based on NIST SP 800-82	1		X	9	6	9	6
	Network Security Architecture for SCADA Systems	1		X	32	21.33	32	21.33
	Implementation of Security Controls for SCADA Systems	1		X	14	9.33	14	9.33
	Developing Resilient and Robust Systems	1	X		5	3.33	5	3.33
	Security testing of SCADA Systems	1	X		28	18.67	28	18.67
Total points		150						
Number of Questions per level of understanding			95	55				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			63.33	36.67				

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.

Taking the Exam

General Information on the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (a national ID card, driver's license, or passport) and show it to the invigilator.

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:

- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB Exam Format and Type

1. **Paper-based:** Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course.
2. **Online:** Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more detailed information about the online format, please refer to the PECB Online Exam Guide.

PECB exams are available in two types:

1. Essay-type question exam
2. Multiple-choice question exam

The exam questions are multiple choice questions: This format has been chosen because it has proven to be effective and efficient for measuring and assessing learning outcomes. The multiple-choice exam can be used to evaluate a candidate's understanding on many subjects, including both simple and complex concepts. Even though the training course contains a lot of factual information, the multiple-choice questions focus on addressing complex thinking skills. When answering these questions, candidates will have to apply various principles, analyze problems, evaluate alternatives, combine several concepts or ideas, etc. Provided that deeper learning and retention is encouraged, the exam will be "closed book." You will find a sample of exam questions provided below.

The use of electronic devices, such as laptops, smartphones, etc., are not allowed.

All attempts to copy, collude, or otherwise cheat during the exam will automatically lead to the failure of the exam.

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

Receiving the Exam Results

Exam results will be communicated via email.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.

- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request a re-evaluation by writing to examination.team@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Any complaint received after 30 days will not be processed.

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

- If a candidate does not pass the exam on the 1st attempt, s/he must wait 15 days after the initial date of the exam for the next attempt (1st retake).

  Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received, because the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

For candidates that fail the exam retake, PECB recommends they attend a training course in order to be better prepared for the exam.

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. Online Exam: when scheduling the exam retake, use initial coupon code to waive the fee
2. Paper-Based Exam: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this policy. The process to schedule the exam retake is the same as for the initial exam.

Closing a Case

If a candidate does not apply for the certificate within three years, their case will be closed. Even though the certification period expires, the candidate has the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, candidate handbook, or exam preparation guide that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing and pay the required fees.

Exam Security

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certificate holders and applicants to maintain the security and confidentiality of PECB exams. If candidates or someone who hold PECB credentials reveal information about PECB exam 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.

Reschedule the Exam

For any changes with regard to the exam date, time, location, or other details, please contact online.exams@pecb.com

Apply for Certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB online profile), including contact details of references who will be contacted to validate the candidate's professional experience. Candidates can submit their application in various languages. Candidates can choose to either pay online or be billed. For additional information, contact certification.team@pecb.com.

The online certification application process is very simple and takes only a few minutes, as follows:

- Register your account
- Check your email for the confirmation link
- Log in to apply for certification

For more information about the application process, follow the instructions on this manual Apply for Certification.

The application is approved as soon as the Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. An email will be sent to the email address provided during the application process to communicate the application status. If approved, candidates will then be able to download the certification from their PECB Account.

PECB provides support in both English and French.

Renew your Certification

PECB certifications are valid for three years. To maintain them, candidates must demonstrate every year that they are still performing tasks that are related to the certification. PECB certified professionals must annually provide Continual Professional Development (CPD) credits and pay $120 as the Annual Maintenance Fee (AMF) to maintain the certification. For more information, please visit the Certification Maintenance page on the PECB website.

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

PECB BEYOND RECOGNITION

Address:
Head Quarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.
T: +1-844-426-7322
F: +1-844-329-7322

PECB Help Center

Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center’s online tracking system. Visit Help Center here: www.pecb.com/help

Emails:
Examination: examination.team@pecb.com
Certification: certification.team@pecb.com
Customer Care: customer@pecb.com

www.pecb.com