Certified Wireless IoT Integration Professional (CWIIP-301) Objectives

Introduction

When you pass the CWIIP exam and hold a valid CWISA certification, you earn the CWIIP certification and credits towards the CWISE certification should you choose to pursue it.

The Certified Wireless IoT Integration Professional (CWIIP) develops and implements solutions that integrate multiple wireless-sourced management, monitoring, and control data through programming. This professional can identify and use the appropriate tools to extract, transform, and load data to and from wireless Internet of Things (IoT) systems. The CWIIP plays a crucial role in planning and delivering scalable solutions to automate the transport of and response to data throughout a heterogeneous network.

The skills and knowledge measured by this examination are derived from a Job Task Analysis (JTA) involving wireless networking experts (CWNEs) and professionals. The results of this JTA were used in weighting the subject areas and ensuring that the weighting is representative of the relative importance of the content.

Subject matter experts (SMEs) involved in the development of these objectives and/or the JTA included:

Robert Bartz, Rowell Dionicio, Troy Martin, Andrew Pandalfino, and Jonathan Smith

The following table provides the breakdown of the exam as to the distribution of questions within each knowledge domain.

Knowledge Domain	**Percentage**
Explain and Use Integration Protocols	20%
Perform Requirements Analysis	20%
Develop IoT Integration Solutions	40%
Implement IoT Integration Solutions	10%
Maintain and Support IoT Integration Solutions	10%

CWNP Authorized Materials Use Policy

CWNP does not condone the use of unauthorized 'training materials' such as 'brain dumps'. Individuals who utilize such materials to pass CWNP exams will have their certifications revoked. In an effort to more clearly communicate CWNP's policy on use of unauthorized study materials, CWNP directs all certification candidates to the CWNP Candidate Conduct Policy at:

http://www.cwnp.com/wp-content/uploads/pdf/CWNPCandidateConductPolicy.pdf

Please review this policy before beginning the study process for any CWNP exam. Candidates will be required to state that they understand and have abided by this policy at the time of exam delivery. If a candidate has a question as to whether study materials are considered "brain dumps", he/she should perform a search using CertGuard's engine, found here: http://www.certguard.com/search.asp

1.0 Explain and Use Integration Protocols (20%)

1.1 Demonstrate proficiency in selecting the best use of integration solutions for wireless IoT implementations

- SNMP
- Publish-subscribe network protocol (MQTT)
- Serialized structured data (gRPC)
- APIs
  - RESTful
  - Web sockets
  - Webhooks
  - Standard HTTP GET/POST/PUT/UPDATE/DELETE processing
- OpenConfig
- FTP / TFTP

1.2 Compare and contrast streaming and polling methods

2.0 Perform Requirements Analysis (20%)

2.1 Identify business requirements and constraints

- Regulatory
- Budgetary
- Legal
- Business use cases
  - Alerting
  - Reporting
  - Response
- Collaborate with internal teams and external partners

2.2 Identify technical requirements and constraints

- Data considerations
  - Retention
  - Capacity
  - Regulatory
  - Confidentiality, Integrity, Availability (CIA)
- Operational considerations

- Monitoring
- Security (Authentication and Authorization)

- Programming languages
- Scalability and Architecture
  - On-premises
  - Cloud
  - Hybrid

2.3 Identify extract, transform, and load (ETL) requirements

3.0 Develop IoT Integration Solutions (40%)

3.1 Demonstrate proficiency with Python

- Interface with an API
- Utilize Dictionaries, Lists, Tuples, and Arrays
- Utilize libraries
- Utilize conditional loops
- Search and isolate unstructured data
  - Regular Expressions (regex)

3.2 Process data contained in commonly used IoT data structures

- JSON
- XML
- YANG
- YAML
- CSV

3.3 Understand and interact with database systems

- Structured
  - Advantages / Disadvantages
  - SQL Queries
  - Tables
  - Primary and foreign key relationships
- Document store
  - Advantages / Disadvantages
  - Queries

- Collections
- Big data
  - Hadoop
  - Streaming

3.4 Understand and implement security methods

- Authentication and Authorization
- Encryption
- IPSec
- HTTPS
- SSL / TLS
- SSH

3.5 Troubleshoot problem scenarios

- Response codes
- Error-handling and exceptions

4.0 Implement IoT Integration Solutions (10%)

4.1 Implement a method to display, monitor, and provide alerts

- Time series data visualization and dashboards
  - Business intelligence reports
  - Technical system health and performance
  - Operational state
- Mechanism for alert communication
  - SMS
  - Email
  - Team collaboration
  - Pager
  - Support ticket system

4.2 Implement automation to provision, configure, and interact with IoT devices

- API
- OpenConfig
- SNMP
- FTP / TFTP

- CLI

5.0 Maintain and Support IoT Integration Solutions (10%)

5.1 Utilize Git for version control

5.2 Continued software maintenance (package managers)

5.3 Documentation

- Develop documentation
- Documentation lifecycle

5.4 Perform validation

- Regression testing
- Unit testing
- Refactoring

5.5 Project lifecycle management

- Scope management
- Change management

5.6 Utilize best practices and methodologies

- Understand security best practices
- Understand software engineering methodologies
- Python enhancement proposals (PEP)

5.7 Be familiar with industry organizations

- IETF
- 3GPP
- Bluetooth SIG
- Zigbee Alliance
- LoRa Alliance
- IEEE
- Z-Wave Alliance