Certified Wireless IoT Design Professional (CWIDP-401) Objectives

Introduction

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

The Certified Wireless IoT Design Professional (CWIDP) has the knowledge and skill set required to define, design, validate and assess wireless IoT solutions. This professional gathers and defines requirements in collaboration with the appropriate stakeholders in order to design wireless IoT networks and related infrastructure with appropriate security considerations. The CWIDP creates design documentation to support the deployment of the required system components and future operations.

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

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

Robert Bartz, Ian Beyer, Jonathan Davis, Landon Foster, Manon Lessard, Peter Mackenzie, Troy Martin, Scott McNeil, Phil Morgan, Jim Palmer, and Djamel Ramoul

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

Knowledge Domain	Percentage
Assess an Existing IoT Solution	5%
Gather and Define Requirements and Constraints	30%
Design a Wireless IoT Solution to Meet Requirements	40%
Validate and Optimize the Wireless IoT Solution	25%

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 Assess an Existing IoT Solution – 5%

1.1 Evaluate an existing IoT implementation and understand its impact on a new wireless IoT deployment

1.2 Use appropriate tools to analyze existing IoT implementations

- 1.2.1 Protocol analyzers (wired and wireless)
- 1.2.2 Spectrum analyzers
- 1.2.3 Network diagrams

1.3 Gather system documentation for the existing IoT solution

1.4 Evaluate operational parameters

- 1.4.1 Wireless signal coverage
- 1.4.2 Frequencies used
- 1.4.3 Functionality
  - Network servers and services used
  - Protocols implemented
- 1.4.4 Potential impact on new deployments

1.5 Document findings for use in the design of the new wireless IoT solution

2.0 Gather and Define Requirements and Constraints – 30%

2.1 Gather business requirements and constraints

- 2.1.1 Use cases and justification
- 2.1.2 Identify coverage areas
- 2.1.3 Budget and schedule
- 2.1.4 Architectural and aesthetic constraints
- 2.1.5 Industry and regulatory compliance
  - Government organizations
  - Standards organizations
  - Certification bodies
  - Occupational Health and Safety
  - Building codes and safety codes
  - Data privacy regulations
- 2.1.6 Data/event collection and control requirements
- 2.1.7 Integration requirements

2.2 Gather technical requirements and constraints

2.2.1 Obtain, create, and validate site plans

2.2.2 Gather environment characteristics and RF measurements

2.2.3 Define device and application data requirements for each area (requirement areas)

2.2.4 Gather and define system requirements

- Network topology, capacity, and redundancy
- Wireless IoT architecture
- IoT technologies aligned with requirements
- Location services (geofencing, asset tracking, etc.)
- Duty cycle, power consumption, and energy harvesting requirements
- Security requirements
- Environment conditions
- Node and tag types and capabilities
- Device mobility
- Vendor selection

2.2.5 Gather and define operational requirements

- System monitoring
- Data collection parameters
- IoT upgrade requirements, when applicable

2.2.6 Gather and define network infrastructure requirements of the planned wireless IoT solution

2.2.7 Gather and define cabling infrastructure requirements of the planned wireless IoT solution

2.2.8 Document existing wireless systems, designs, and related documentation, when applicable

3.0 Design a Wireless IoT Solution to Meet Requirements – 40%

3.1 Design for the selected topologies

3.1.1 Mesh

3.1.2 PtP

3.1.3 PtMP

3.1.4 P2P

3.1.5 Tree

3.1.6 Star

3.1.7 Cluster Tree

3.2 Design for appropriate channel configuration

3.6.1 Channel selection

3.6.2 Channel and protocol functionality

- Bandwidth
- Dwell time
- Spread factor
- Superframes
- Modulation and coding

3.6.3 Blocklist or blocked channels

3.3 Design based on RF requirements and capabilities

3.3.1 Use RF measurements and survey tools
3.3.2 Use RF modeling tools
3.3.3 Perform continuous wave (CW) testing
3.3.4 Perform onsite coverage testing/Proof of Concept (PoC)

3.4 Use wireless IoT tools to create and validate the design

3.3.1 Generate a predictive RF model using wireless design tools

- Import and scale plans (floor, map)
- Import geodata (outdoor design)
- Model attenuation based on calibration
- Select and place nodes
- Define requirement areas and parameters

3.3.2 Use additional tools to assist in the design process

- RF modeling tools
- Distance measuring tools
- Cable testers
- Protocol capture and analysis tools
- Cameras
- Power kits
- Diagramming tools
- Personal Protective Equipment (PPE)
- PoC kit (customer devices, gateways, coordinators, sensors, actuators, tags, etc.)

3.3.3 Utilize validation tools

- Topology validation
- RF scanners
- Survey software
- Spectrum analyzers

3.5 Produce or recommend designs and configuration parameters for the IoT-related network infrastructure requirements

3.5.1 Required infrastructure hardware and software

- Application servers
- Data storage
- Big data systems
- Join servers
- Cloud platforms
- Containers
- Switches
- Gateways/Coordinators
- Network backhaul

3.5.2 Required PoE and power budgets

3.5.3 Recommend robust security solutions

- Authentication
- Join Keys
- Encryption
- Privacy
- Access Control Lists
- Firewalls
- Segmentation
- Change configuration defaults

3.5.4 Required QoS configuration based on the selected wireless IoT protocol and supported wired network QoS parameters

3.6 Produce design documentation

3.6.1 Bill of Materials (BoM)

3.6.2 Design report

- Heat maps
- Device placement maps
- Cabling runs
- Configuration parameters

3.6.3 Physical installation guide

4.0 Validate and Optimize the Wireless IoT Solution – 25%

4.1 Validate that the RF requirements are met by the solution

4.1.1 Ensure coverage requirements are met

4.1.2 Ensure capacity requirements are met

4.1.3 Identify and resolve interference sources, when applicable

4.2 Validate that the IoT solution is functioning as defined in the solution requirements

4.2.1 Conduct device testing
4.2.2 Conduct mobility testing
4.2.3 Verify proper security configuration and firmware/software support
4.2.4 Verify proper node (or asset tag) and antenna installation per design specifications and location
4.2.5 Verify power and grounding requirements are met
4.2.6 Verify channel selections and transmit power
4.2.7 Verify aesthetic requirements are met

4.3 Recommend and/or perform appropriate corrective actions as needed based on validation results for RF requirements and IoT solution functionality requirements

4.4 Create a validation and test report including solution documentation and asset inventory/asset documentation

4.5 Final meeting (Q&A and hand-off)

CWIDP-401 Exam Acronyms

For the CWIDP-401 exam, you should be able to understand and clearly define the following acronyms in relation to wireless IoT design. Such acronyms may be used on the CWIDP-401 exam without definition.

AAA	Authentication, Authorization, and Accounting
ACI	Adjacent Channel Interference
ACL	Access Control List
AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
AP	Access Point
BLE	Bluetooth Low Energy
CCI	Co-Channel Interference
CIA	Confidentiality, Integrity, and Availability
CoAP	Constrained Application Protocol
CRC	Cyclic Redundancy Check
CW	Continuous Wave
dB	Decibel
dBi	Decibel to Isotropic
dBm	Decibel to Milliwatt
DDS	Data Distribution Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EIRP	Equivalent Isotropically Radiated Power
FCC	Federal Communications Commission
FCS	Frame Check Sequence

FTP	File Transfer Protocol
Gbps	Gigabits Per Second
GBps	Gigabytes Per Second
GHz	Gigahertz
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
Hz	Hertz
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IIoT	Industrial Internet of Things
IP	Internet Protocol
IR	Intentional Radiator
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code (in security context)
MAC	Medium Access Control (in Layer 2 networking context)
Mbps	Megabits Per Second
MBps	Megabytes Per Second
MD5	Message Digest algorithm 5
MDM	Mobile Device Management
MHz	Megahertz
MIC	Message Integrity Check

MITM	Man-in-the-Middle
MQTT	Message Queueing Telemetry Transport
mW	Milliwatt
NAC	Network Access Control
NIC	Network Interface Card
NTP	Network Time Protocol
OTA	Over-the-Air
PD	Powered Device
PHY	Physical Layer
PIN	Personal identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PSE	Power Source Equipment
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RC4	Rivest Cipher 4
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identifier
RSSI	Received Signal Strength Indicator
Rx	Receive or Receiver
SHA2	Secure Hash Algorithm version 2
SHA3	Secure Hash Algorithm version 3
SIEM	Security Information and Event Management
SINR	Signal-to-Interference plus Noise Ratio

SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SOHO	Small Office Home Office
SSH	Secure Shell
STA	Station
TCP	Transmission Control Protocol
Tx	Transmit or Transmitter
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W	Watt
WAN	Wire Area Network
WLAN	Wireless Local Area network