Certified Wireless IoT Connectivity Professional (CWICP-201) Objectives

Introduction

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

The Certified Wireless IoT Connectivity Professional (CWICP) understands IoT connectivity standards and operation in business and industrial networks. This knowledge can be applied to deploy and troubleshoot the most common wireless IoT protocols with an in-depth understanding of their operations. A CWICP should be able to identify the technology and security requirements for a given IoT solution.

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:

Jonathan Davis, Landon Foster, Manon Lessard, Peter Mackenzie, Jennifer Minella, Phil Morgan, 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
Wireless IoT Technologies and Solutions	10%
Wireless IoT RF Characteristics	10%
Wireless IoT PHY Structure and Operations	20%
Wireless IoT MAC Layer Structure and Operations	20%
Wireless IoT Security	10%
Validate and Troubleshoot IoT 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 Wireless Iot Technologies and Solutions (10%)

1.1 Understand wireless IoT architectures

- Understand and apply knowledge of high-level IoT architectures for the purpose of making recommendations on technology/technologies that will fit a requirement, such as:
    - Understand long-range vs short-range technologies
    - Understand mesh
    - PtP/PtMP topologies

1.2 Identify the benefits and constraints of various wireless IoT architectures and technologies

1.3 Understand and apply knowledge of the benefits and constraints/limitations of discrete IoT-related features for the purpose of making recommendations on technologies that will meet a requirement, such as battery life/time, distance, etc.

1.4 Understand wireless IoT components

- Understand and apply knowledge of basic IoT components found throughout most common IoT technologies and architectures such as:
    - Wireless IoT endpoints
    - Wireless IoT gateways
    - Nodes
    - Coordinators
    - IoT routers
    - Devices with IoT components integrated (e.g. APs with integrated IoT gateways)

1.5 Differentiate between component interactions and architectures of specific wireless IoT technologies

- Apply knowledge of architectures and components to compare and contrast common IoT technologies for the purpose of making recommendations for IoT technologies that will meet a specific project/business needs. These architectures and components include:
- LPWANs (LoRa/LoRaWAN, Sigfox),
- 802.15.4 (Zigbee, Thread, ISA100.11a, WirelessHART)

2.0 Wireless IoT RF Characteristics (10%)

2.1 Understand frequency band characteristics

2.2 Understand the characteristics of commonly used IoT frequency bands, specifically 400MHz, 800/900MHz, 2.4GHz

2.3 Concepts and relationships of frequencies to FSPL

2.4 Effect of receive sensitivity on RSSI across various bands (Friis Transmission Equation)

2.5 Incumbents in the airspace

2.6 Propagation characteristics

2.7 Explain channel widths, SNR and other power considerations

2.8 Understand the characteristics of commonly used IoT RF bands
2.9 Relationship of channel widths to SNR (SNR as a function of channel width)
2.10 Rx/Tx power considerations,
2.11 Causes and effects of dynamic range compression and desense

3.0 Wireless IoT PHY Structure and Operations (20%)

3.1 Understand 802.15.4 PHY structure and operations used in IoT

- Understand in-depth and be able to describe wireless IoT-related 802.15.4 PHY:
  - PPDU formats, specifically O-QPSK-PHY, BPSK-PHY, CSS-PHY
  - Bands
  - Channel widths and spacing
  - Modulation, encoding, and data rates
  - Error correction

3.2 Understand LoRa PHY structure and operations

- Understand in-depth and be able to describe LoRa PHY:
  - Bands
  - Channel widths and spacing
  - Modulation, encoding, and data rates
  - Error correction
  - CSS (Chirp Spread Spectrum)
  - Spreading Factor (SF)
  - Adaptive Data Rate (ADR)
  - Uplink/downlink messages

3.3 Understand Sigfox PHY structure

- Understand high-level concepts of Sigfox PHY such as:
  - Bands and use of ultra-narrow band (UNB)
  - Channel widths and spacing,
  - Modulation, encoding, and data rates
  - Error correction

3.4 Understand Z-Wave PHY structure

- Understand high-level concepts of Z-Wave PHY such as:
  - Bands
  - Channel widths and spacing
  - Modulation, encoding, and data rates
  - Error correction

3.5 Understand Bluetooth PHY structure and operations used in IoT

- Understand high-level concepts of Bluetooth PHY such as:
  - Bluetooth Basic Rate (BR) and Enhanced Data Rate (EDR)
  - Bands

    - Channel widths and spacing
    - Modulation, encoding, and data rates
    - Error correction

3.6 Understand Bluetooth Low Energy (BLE) PHY structure and operations used in IoT

- Understand in-depth and be able to describe Bluetooth Low Energy (BLE) PHY such as:
    - Bands
    - Channel widths and spacing
    - Advertisement Channels (37-39), Data Channels (0-36)
    - Modulation, encoding, and data rates
    - Error correction

4.0 Wireless IoT MAC Layer Structure and Operations (20%)

4.1 Understand 802.15.4 MAC layer structure and operations for IoT

- Understand MAC Frame Format of 802.15.4 including Frame control, Sequence Numbers, PAN ID, Address Fields, IEs, PAN ID Compression, TDMA/GTS
- Understand MAC Frame types of 802.15.4 including Beacon, Data, Ack, MAC Command, Multipurpose, Fragment, Extended
- Understand 802.15.4 MAC Operations including MAC Management Services, MAC Data Service, MAC Constants and PIB Attributes

4.2 Understand LoRaWAN MAC layer structure and operations for IoT

- LoRa MAC frame format, MAC Header (HDFR), MAC Payload, Encryption
- Understand the classes of MAC operation in LoRaWAN including Class A (Baseline), Class B (Beacon), Class C (Continuous) and Aloha operation in LoRaWAN
- Message Types in LoRaWAN
- MAC Commands in LoRaWAN
- Activation in LoRaWAN

4.3 Understand Bluetooth Low Energy (BLE) MAC layer structure and operations for IoT

- BLE connectivity concepts and MAC operations

5.0 Wireless IoT Upper Layers Protocols (20%)

5.1 Understand Zigbee upper layer protocols network topology including:

- Addressing scheme
- Ad-hoc on-demand Distance Vector Routing Protocol (AODV)
- Discovery methodologies, device roles
- Zigbee Device Object (ZDO)
- Application Framework
- Application Support Sublayer
- Application and Device Profiles

5.2 Understand 6LoWPAN upper layer protocols

- Basic IPv6 addressing concepts
- ICMP v6
- LoWPAN Adaptation Layer and relevant/implemented frame formats
- Mesh addressing
- Mesh Header option

5.3 Understand Thread upper layer protocols

- Device types and network structure
- Mesh link establishment
- Message forwarding and routing
- Router Selection
- Security
- Mesh Commissioning Protocol

5.4 Understand WirelessHART and ISA100.11a upper layer protocols

- Understand the similarities and differences between WirelessHART and ISA100.11a
- Understand the WirelessHART encapsulation protocol including:
    - MAC frame formats (superframes)

5.5 Understand ISA100.11a Data Link and Network layer interactions and operations, including:

- IAS100.11a Data Link (MAC sub-layer & Upper layer data link sub-layer)
- MAC frame formats
- Network Layer (NLMO and NPDU)
- Network Addressing

6.0 Wireless IoT Security (10%)

6.1 Understand and apply IoT privacy and integrity concepts

- Understand and apply knowledge of IoT security primitives including:
    - Secure key exchanges
    - Lightweight encryption algorithms for IoT
    - Commonly used hashing algorithms in IoT
- Be able to compare and select appropriate encryption components (e.g. key length, algorithm strength, etc.) based on security requirements of the IoT solution or business requirement

6.2 Understand and apply secure provisioning & access control in IoT

- Understand risks and vulnerabilities related to provisioning IoT components (e.g. endpoints, gateways, routers)
- Understand the required security for a given IoT solution or business requirement
- Understand and apply mitigations for risks related to provisioning including proper authentication and authorization of devices allowed to access/join the IoT network

6.3 Implement IoT technology against a defined security policy

6.4 Implement network segmentation as required including:

- Demonstrate the ability to properly segment IoT networks or components for security, as defined by best or common practices
- Dynamic ACLs
- VLANs
- Air gap
- Firewall

6.5 Understand the different security requirements of data-centric vs. action-centric IoT solutions

- Implement applied knowledge of the IoT components as it relates to their ability to collect, pass, process data OR to take an action, both of which may have different levels of security requirements
- Understand the IoT system and security risks and requirements and inform the stakeholders and designers

7.0 Validate and Troubleshoot Wireless IoT Solutions (10%)

7.1 Identify and solve common IoT issues and/or misconfiguration

- Use of the following tools for the purposes of testing and troubleshooting connectivity of wireless IoT networks and components including
  - Protocol analyzer
  - Spectrum analyzer
  - USB dongles
  - Development boards
  - RF testers
  - Protocol-specific apps
  - Vendor-specific utilities

7.2 Demonstrate applied knowledge of the IoT-related PHY, MAC, and upper layers concepts for troubleshooting and configuration changes when required

7.3 Validate against a defined set of requirements

- Proficient use of validation tools and processes including
- Spectrum analyzer
- Heatmaps tools
- Data path validation
- Application of processes for the purpose of validating against a predefined set of requirements.

7.4 Validate against recommended best practices

- Maintain knowledge of vendor, industry, and technology best practices where to find these resources

- Prove the ability to research vendor documentation and FCC or other regulatory domain authority radio databases for the purposes of validating an IoT network and components against best practices