Certified Wireless IoT Solutions Administrator (CWISA-102) Objectives

Introduction

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

The Certified Wireless IoT Solutions Administrator (CWISA) implements, administers and troubleshoots technologies that heavily rely upon, or directly integrate with, wireless systems in enterprise, government, and manufacturing environments. This individual can install, customize, and coordinate appropriate solutions to meet an organization's requirements and constraints.

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 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 original JTA included:

Ryan Adzima, Robert Bartz, Ian Beyer, Tom Carpenter, Joshua Gochee, Bryan Harkins, Jason Hintersteiner, and Manon Lessard

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

Knowledge Domain	Percentage
Wireless Technologies	15%
Radio Frequency Communications	15%
Planning Wireless Solutions	20%
Implementing Wireless Solutions	25%
Supporting Wireless Solutions	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 Wireless Technologies (15%)

- 1.1 Maintain continued awareness of wireless IoT technologies and applications of those technologies
  - 1.1.1 Understand research and lab testing skills to maintain technology awareness
  - 1.1.2 Understand the most common applications of wireless technologies, the frequencies used and communication protocols
- 1.2 Understand industry standard, certification and regulatory organizations and standards development processes
  - 1.2.1 Institute of Electrical and Electronics Engineers (IEEE)
  - 1.2.2 Internet Engineering Task Force (IETF)
  - 1.2.3 Wi-Fi Alliance
  - 1.2.4 International Telecommunication Union (ITU)
  - 1.2.5 Bluetooth Special Interest Group (SIG)
  - 1.2.6 3rd Generation Partnership Project (3GPP)
  - 1.2.7 Connectivity Standards Alliance (CSA)
  - 1.2.8 LoRa Alliance
  - 1.2.9 Explain the roles of regulatory agencies such as the FCC, IC, CE and others
- 1.3 Define wireless network types
  - 1.3.1 Wireless Local Area Network (WLAN)
  - 1.3.2 Wireless Personal Area Network (WPAN)
  - 1.3.3 Wireless Body Area Network (WBAN)
  - 1.3.4 Wireless Metropolitan Area Network (WMAN)
  - 1.3.5 Wireless Wide Area Network (WWAN)
  - 1.3.6 Wireless Sensor Network (WSN)
  - 1.3.7 Internet of Things (IoT)
    - 1.3.7.1 Industry 4.0/5.0
    - 1.3.7.2 Connected Vehicles
    - 1.3.7.3 Smart Cities
    - 1.3.7.4 Smart Offices/Buildings/Homes
- 1.4 Understand hardware and software components of IoT end devices and gateways
  - 1.4.1 Processors
  - 1.4.2 Memory
  - 1.4.3 Radios
  - 1.4.4 Storage
  - 1.4.5 Sensors
  - 1.4.6 Network connections
  - 1.4.7 Operating Systems/Firmware
  - 1.4.8 Application/Service Software

- 1.4.9 Off-the-shelf Devices
- 1.4.10 Custom Devices

2.0 Radio Frequency Communications (15%)

- 2.1 Explain the basic RF wave characteristics, behaviors and measurements used for wireless communications
  - 2.1.1 Frequency, wavelength, amplitude, and phase
  - 2.1.2 Amplification, attenuation, and free space path loss
  - 2.1.3 Absorption, reflection, refraction, scattering, and diffraction
  - 2.1.4 RF signal metrics
    - 2.1.4.1 Watt, milliwatt, and microwatt
    - 2.1.4.2 Decibel (dB) and decibels to milliwatt (dBm)
    - 2.1.4.3 RF noise and noise floor
    - 2.1.4.4 SNR and SINR
- 2.2 Describe the fundamentals of modulation techniques used in wireless communications
  - 2.2.1 Amplitude Shift Keying (ASK)
  - 2.2.2 Frequency Shift Keying (FSK)
  - 2.2.3 Phase Shift Keying (PSK)
  - 2.2.4 Amplitude and Phase Shift Keying (APSK)
  - 2.2.5 Quadrature Amplitude Modulation (QAM)
  - 2.2.6 Orthogonal Frequency Division Multiplexing (OFDM)
  - 2.2.7 Orthogonal Frequency Division Multiple Access (OFDMA)
  - 2.2.8 Frequency Hopping
  - 2.2.9 Chirp Spread Spectrum (CSS)
  - 2.2.10 Additional modulation methods (AM, FM, and CW)
- 2.3 Explain the basic capabilities of components used in RF communications
  - 2.3.1 Radios (receivers, transmitters, and transceivers)
  - 2.3.2 Antennas
  - 2.3.3 Intentional radiator and Equivalent Isotropically Radiated Power (EIRP) and Effective Radiated Power (ERP)
  - 2.3.4 RF cabling and connectors
  - 2.3.5 Link types including PTP, PTMP, mesh, ad-hoc and on-demand
- 2.4 Describe the basic use and capabilities of the RF bands
  - 2.4.1 Radio Frequency Bands
  - 2.4.2 RF bands and communication ranges
  - 2.4.3 RF bands and power levels

3.0 Planning Wireless Solutions (20%)

- 3.1 Identify and use the wireless IoT system requirements
  - 3.1.1 Use cases and applications
  - 3.1.2 Capacity requirements
  - 3.1.3 Security and monitoring requirements
  - 3.1.4 Integration requirements (automation, data transfer/conversion, APIs, cross-platform integration)
  - 3.1.5 Stakeholder identification
- 3.2 Identify and comply with system constraints
  - 3.2.1 Budgetary constraints
  - 3.2.2 Security constraints
  - 3.2.3 Technical constraints
  - 3.2.4 Business policies and requirements
  - 3.2.5 Regulatory constraints
  - 3.2.6 System dependencies
  - 3.2.7 Evaluate existing network infrastructure and understand its limitations in the context of the new wireless system
- 3.3 Select appropriate wireless IoT solutions based on requirements and constraints
- 3.4 Plan for the technical requirements of the wireless IoT solution
  - 3.4.1 LAN networking requirements (VLANs, PoE, TCP/IP, DHCP, DNS, wired connectivity, cellular connections, serial data)
  - 3.4.2 WAN networking requirements
  - 3.4.3 Systems requirements (virtualization, containers, cloud platforms, cabling, grounding, radios, antennas)
  - 3.4.4 APIs, protocols, and programmability (RESTful, Webhooks, Web Sockets, OpenConfig, MQTT)
  - 3.4.5 Frequency coordination compliance (channel capacity management, interoperability, interference management)
- 3.5 Understand the basic features and capabilities of common wireless IoT solutions and plan for their implementation
  - 3.5.1 Internet of Things (IoT) (CO-to-CO, CO-to-Service, CO-to-human)
  - 3.5.2 802.11 WLANs
  - 3.5.3 Bluetooth
  - 3.5.4 Zigbee
  - 3.5.5 802.15.4-based protocols
  - 3.5.6 LoRaWAN
  - 3.5.7 Sigfox

3.5.8 Location services (RTLS, Bluedot, geofencing, beaconing) and location methods, including triangulation, trilateration and multi-lateration

4.0 Implementing Wireless Solutions (25%)

4.1 Understand the wireless IoT solution and consider key issues related to automation, integration, monitoring, and management
- 4.1.1 Automation, integration, and management protocols and standards (APIs, programming languages, data structures, communication protocols, data of interest, analytics, and services)
- 4.1.2 Monitoring solutions (integrated, overlay, APIs)

4.2 Use best practices in wireless IoT solution implementations
- 4.2.1 Pilot testing (proof-of-concept, early-stage analysis)
- 4.2.2 Configuration and staging
- 4.2.3 Installation
- 4.2.4 Documentation

4.3 Validate wireless solution implementations including RF communications and application functionality
- 4.3.1 Initial testing
- 4.3.2 Troubleshooting and remediation

4.4 Understand and implement basic installation procedures
- 4.4.1 Configure and mount wireless equipment according to applicable safety requirements (OSHA) and building codes
- 4.4.2 Configure connectivity (wireless and wired)
- 4.4.3 Configure the network infrastructure or communicate configuration requirements to the appropriate individuals
- 4.4.4 Configure cloud connectivity where appropriate
- 4.4.5 Configure features related to video, voice, captive portals, container-based apps, telemetry, location services, MDM and SDN/NFV
- 4.4.6 Implement appropriate security solutions for the selected wireless system
  - 4.4.6.1 Authentication
  - 4.4.6.2 Authorization
  - 4.4.6.3 Encryption
  - 4.4.6.4 Monitoring

4.5 Implement best practices in knowledge transfer and hand-off
- 4.5.1 Staff training (end users, administrators)
- 4.5.2 Solution documentation (topology, configuration, protocols, physical locations, APIs in use)

4.5.3 Final customer meeting (requirements review, stakeholder approval)

5.0 Supporting Wireless Solutions (25%)

5.1 Administer the wireless solution while considering the implications of various vertical markets
- 5.1.1 Healthcare
- 5.1.2 Industrial/Manufacturing
- 5.1.3 Smart Cities
- 5.1.4 Consumer spaces (smart homes)
- 5.1.5 Smart Agro
- 5.1.6 Smart Offices/Buildings
- 5.1.7 Retail
- 5.1.8 Education
- 5.1.9 Large Public Venues

5.2 Troubleshoot common problems in wireless IoT solutions
- 5.2.1 Interference
- 5.2.2 Improper configuration
- 5.2.3 Security misconfiguration
- 5.2.4 Signal strength
- 5.2.5 Malfunctioning hardware
- 5.2.6 Software/firmware issues
- 5.2.7 Drivers
- 5.2.8 Faulty custom software code
- 5.2.9 Faulty installation

5.3 Understand and determine the best use of scripting and programming solutions for wireless IoT implementations
- 5.3.1 Identify and differentiate among the features of various scripting/programming languages (Python, R, PHP, C (and variants), JavaScript, Java and TypeScript)
- 5.3.2 Understand the basics of data structures commonly used for integration of networked systems
  - 5.3.2.1 JSON
  - 5.3.2.2 YANG
  - 5.3.2.3 XML
  - 5.3.2.4 YAML
  - 5.3.2.5 XAML
- 5.3.3 Understand the basics of APIs and common models
  - 5.3.3.1 RESTful
  - 5.3.3.2 webhooks

5.3.3.3 WebSockets
5.3.3.4 Standard HTTP GET/POST processing

5.3.4 Understand the basics of networking, application and security protocols used in wireless IoT solutions
5.3.4.1 HTTP/HTTPS
5.3.4.2 NETCONF
5.3.4.3 OpenConfig
5.3.4.4 MQTT, DDS, AMQP, CoAP
5.3.4.5 SNMP
5.3.4.6 SSL/TLS
5.3.4.7 SSH
5.3.4.8 IPv4/IPv6
5.3.4.9 TCP/UDP

5.4 Understand application architectures and their impact on wireless IoT solutions
5.4.1 Single-tier architecture
5.4.2 Multi-tier architecture
5.4.3 Database systems (relational, No-SQL, streaming data)
5.4.4 Web Servers
5.4.5 Application servers/services (Network Time Protocol, DNS, system-specific)