

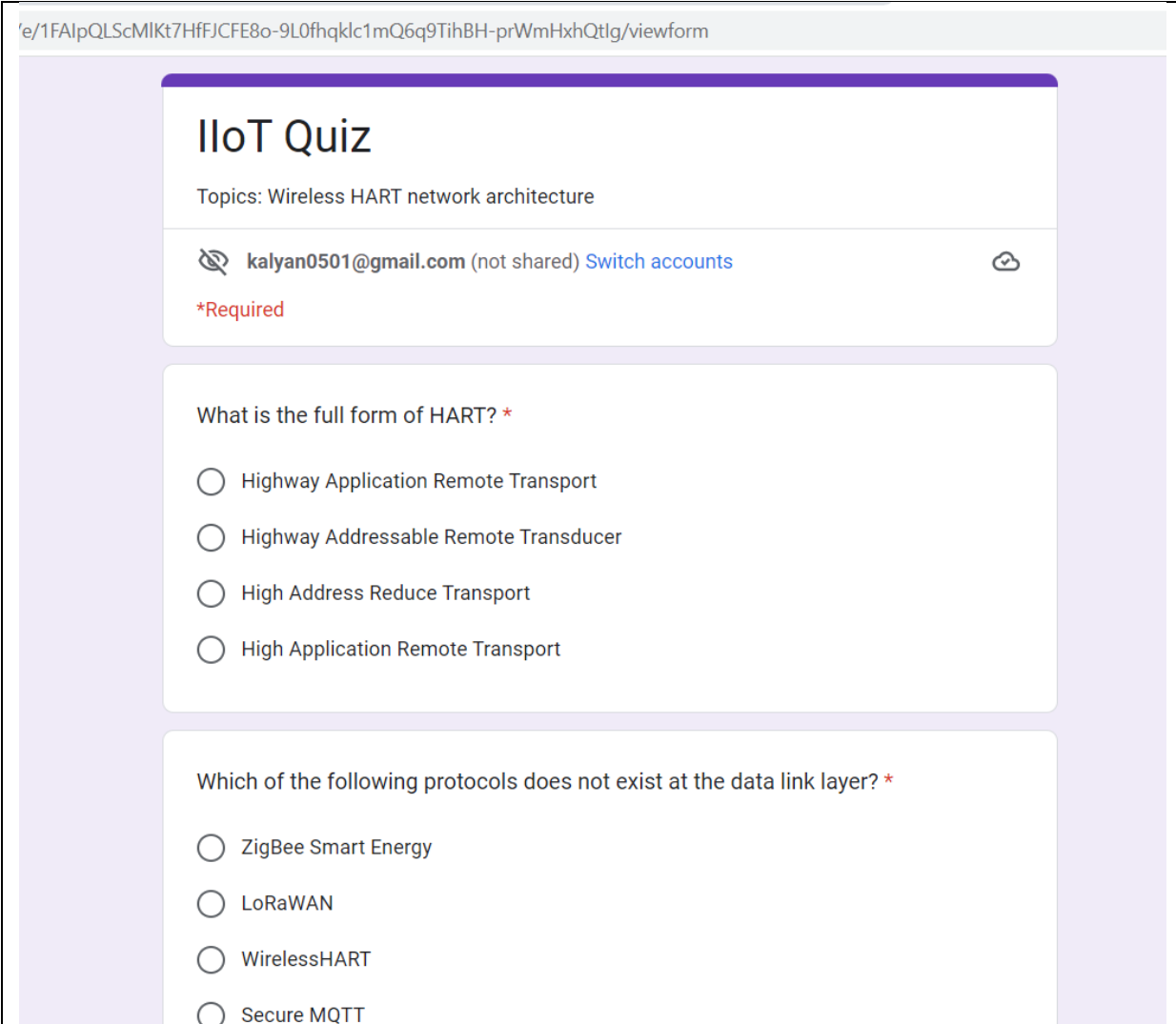
Introduction to Internet of things

P.Surendra, Assistant Professor, Information Technology, Aditya Engineering College,
Surampalem.

Subject: Introduction to Internet of Things

Topic: Wireless HART network architecture

Teaching Methodology: Quiz



The image shows a screenshot of a Google Forms quiz titled "IIoT Quiz". The form is displayed in a browser window with the URL `'e/1FAIpQLScMIkt7HfFJCFE8o-9L0fhqklc1mQ6q9TihBH-prWmHxhQtIg/viewform`. The quiz title is "IIoT Quiz" and the topic is "Wireless HART network architecture". The user is identified as `kalyan0501@gmail.com` (not shared) with a "Switch accounts" link. A red asterisk indicates that the email is required. The quiz contains two questions, both marked as required with a red asterisk. The first question is "What is the full form of HART? *" with four radio button options: "Highway Application Remote Transport", "Highway Addressable Remote Transducer", "High Address Reduce Transport", and "High Application Remote Transport". The second question is "Which of the following protocols does not exist at the data link layer? *" with four radio button options: "ZigBee Smart Energy", "LoRaWAN", "WirelessHART", and "Secure MQTT".

Fig.1. Quiz

<https://forms.gle/juwfUXAA7DoWG2Dx8>

Marks:

| Sl.No | Roll.No | Student Name | marks |
|-------|------------|---|-------|
| 1 | 20A91A1201 | ADABALA HANI GANGA BHAVANI | 2 |
| 2 | 20A91A1202 | ANGULURI KAVYA SHREE | 1 |
| 3 | 20A91A1203 | ANKAM VEERA SATYA GANGA VENI | 10 |
| 4 | 20A91A1204 | ARETI RENUKA | 7 |
| 5 | 20A91A1205 | B SUNITA | 3 |
| 6 | 20A91A1206 | BIRADA VENKATA SAI MANASWITHA | 2 |
| 7 | 20A91A1207 | CHALUVADI SAI DEVI AISHWARYA | 1 |
| 8 | 20A91A1208 | CHEKURI LEKYA SRI | 2 |
| 9 | 20A91A1209 | CHILUKURI SANJU | 10 |
| 10 | 20A91A1210 | D S VENKATANARAYANA RAO MUTYAM | 6 |
| 11 | 20A91A1211 | DIGHVIJAY SINGH CHAUHAN | 2 |
| 12 | 20A91A1212 | ELURI VASAVI | 1 |
| 13 | 20A91A1213 | GOSIPATHA VASU | 8 |
| 14 | 20A91A1214 | GRANDHI BHARGAVA SAI | 2 |
| 15 | 20A91A1215 | INDUGAPALLI KARTHEEK | 8 |
| 16 | 20A91A1216 | JALLEPALLI PRASUNA CHANDRIKA | 4 |
| 17 | 20A91A1217 | JAVVADI VENKATA KEERTHI SRI NAGA KUMARI | 5 |
| 18 | 20A91A1218 | KADALI LAXMIVINEELA | 4 |
| 19 | 20A91A1219 | KANIGICHERLA VENKATA NAGA DURGA SREYA | 7 |
| 20 | 20A91A1220 | KANURI GEETHA PRAVALLIKA | 3 |
| 21 | 20A91A1221 | KARRI PRADEEP KUMAR | 6 |
| 22 | 20A91A1222 | KOLUKULA ROHINI PRIYA | 4 |
| 23 | 20A91A1223 | KONJARLA REKHA BHAVYA POORNIMA | 1 |
| 24 | 20A91A1224 | MADDIPATI ANIL SRI KRISHNA | 7 |
| 25 | 20A91A1225 | MADDIPATI NAGA HARSHITHA | 2 |
| 26 | 20A91A1226 | MADDUKURI GNANA GITA PRASANTI | 8 |
| 27 | 20A91A1227 | MADENA SRIVARSHINI | 2 |
| 28 | 20A91A1228 | MAILAPALLI PRAVEEN | 4 |
| 29 | 20A91A1229 | MANURI BHAVYA DEEPIKA | 8 |
| 30 | 20A91A1230 | MEDABOINA VIJAYKANTH | 10 |
| 31 | 20A91A1231 | MEDAPATI DHANA VEERA SUBHADRA LAKSHMI | 1 |
| 32 | 20A91A1232 | MUJAVAR MALIKBASHA | 8 |
| 33 | 20A91A1233 | NALLALA CHAKRAVARTHI | 4 |
| 34 | 20A91A1234 | NARAKULA BHASKARA NARASIMHA SIVA GOWTHAM | 7 |

| | | | |
|----|------------|--|----|
| 35 | 20A91A1235 | NARIGIRI SRINIVASA S S MANI VINAY KUMAR | 10 |
| 36 | 20A91A1236 | NAVEEN KUDELLI | 1 |
| 37 | 20A91A1237 | NEPALA UDAY KIRAN | 3 |
| 38 | 20A91A1238 | PABBIREDDY AKANKSHA | 7 |
| 39 | 20A91A1239 | PADALA VENKATA KRISHNA REDDY | 2 |
| 40 | 20A91A1240 | PADILAM SANTHOSH MANIKANTA | 4 |
| 41 | 20A91A1241 | PALACHARLA CHANDRA RISHIK | 5 |
| 42 | 20A91A1242 | PALLIBHATLA LAHARI SREEDHA | 3 |
| 43 | 20A91A1243 | PATURI SUDEEP KUMAR | 8 |
| 44 | 20A91A1244 | PIRADULA ANITHA | 3 |
| 45 | 20A91A1246 | POOJITHA BONTHU | 1 |
| 46 | 20A91A1247 | POTHAMSETTI VENKATA SAI RAMA REDDY | 1 |
| 47 | 20A91A1248 | POTNURI MAHESH | 9 |
| 48 | 20A91A1249 | MUKESH KUMAR SAH | 8 |
| 49 | 20A91A1250 | ROUTHU NAGA SHIVA MANOHAR | 5 |
| 50 | 20A91A1251 | SHAIK FAYAZ | 2 |
| 51 | 20A91A1252 | TALARI UDAY BHASKAR | 8 |
| 52 | 20A91A1253 | VADDADI YESWANTH SAI | 2 |
| 53 | 20A91A1254 | VANAPARTHI B V M GOVINDARAJ | 3 |
| 54 | 20A91A1255 | VANKADARA NAVYA | 5 |
| 55 | 20A91A1256 | VELAGALA SAI NITHIN REDDY | 5 |
| 56 | 20A91A1257 | VUKKUM SAJEEVA KUMARI | 4 |
| 57 | 20A91A1258 | VUTA NAGA JAYA LAKSHMI | 4 |
| 58 | 20A91A1259 | YALAKA SRIKANTH | 9 |
| 59 | 20A91A1260 | YANDAMURI NISCHALA | 8 |
| 60 | 20A91A1261 | YARRAMSETTY JAYADEEP | 3 |
| 61 | 20A91A1263 | SHUBHAM KUMAR RAJ | 6 |
| 62 | 20A91A1264 | KANCHARLA CHARAN | 7 |
| 63 | 20A91A1265 | DHIRAJ GUPTA | 7 |
| 64 | 21A95A1201 | KARELLA HARI VENKATA RAVI CHANDRA | 8 |
| 65 | 21A95A1202 | KONA S V K PRIYANKA | 8 |
| 66 | 21A95A1203 | MADDA NAVEEN JOSEPH | 2 |
| 67 | 21A95A1204 | NATLA PRIYANKA | 4 |
| 68 | 21A95A1205 | PANCHADI SAI SUDHA | 9 |
| 69 | 21A95A1206 | SINGULURI DINESH | 7 |
| 70 | 21A95A1207 | VASAMSETTY MOHAN SAI VENKAT | 2 |

Wireless HART network

Wireless HART Communication Protocol Overview

by Editorial Staff

As the need for additional process measurements increases, users seek a simple, reliable, secure and cost-effective method to deliver new measurement values to control systems without the need to run more wires. With process improvements, plant expansions, regulatory requirements and safety levels demands for additional measurements, users are looking to wireless technology for that solution.

With approximately 30 million HART devices installed and in service worldwide, HART technology is the most widely used field communication protocol for intelligent process instrumentation. With the additional capability of wireless communication, the legacy of benefits this powerful technology provides continues to deliver the operational insight users need to remain competitive.

Wireless HART

Backed by the Power of HART

- Built on proven industry standards
- Created by industry and technology experts
- Multi-vendor support and interoperable devices
- Uses existing devices, tools and knowledge

Flexible Applications

- Reduced installation costs – no wires!
- Process monitoring, control and asset management
- Health, safety and environmental compliance monitoring

Supports All Phases of the Plant Life Cycle

- Fast engineering, deployment and commissioning
- Cost-effective move from scheduled to predictive maintenance
- Easy diagnosing and troubleshooting

Simple. Reliable. Secure.

Even though millions of HART devices are installed worldwide, in most cases the valuable information they can provide is stranded in the devices. An estimated 85% of all installed HART devices are not being accessed to deliver device diagnostics information with only the Process Variable data communicated via the 4-20mA analog signal. This is often due to the cost and the difficulty of accessing the HART information.

*Wireless*HART technology allows users to access the vast amount of unused information stranded in these installed HART smart devices—85% of the installed HART devices. It also provides a *simple, reliable* and *secure* way to deploy new points of measurement and control without the wiring costs.

1. Simple

WirelessHART is a robust technology that is simple to implement. It enables users to quickly and easily gain the benefits of wireless technology while maintaining compatibility with existing HART devices, tools and systems.

Easy Installation and Commissioning

- Familiar tools, work flow and procedures
- Multiple power options
- Reduced installation and wiring costs
- Coexistence with other wireless networks
- Supports both star and mesh topologies
- Add devices one at a time

Automatic Network Features

- Self-organizing and self-healing
- Always-on security
- Adjusts as new instruments are added
- Adjusts to changes in plant infrastructure

2. Reliable

Industrial facilities with dense infrastructures, frequent movement of large equipment, changing conditions, or numerous sources of radio-frequency and electromagnetic interference may have communication challenges. *WirelessHART* includes several features to provide built-in 99.9% end-to-end reliability in all industrial environments.

Standard Radio with Channel Hopping

- Radios comply with IEEE 802.15.4-2006
- 2.4GHz license free frequency band
- “Hops” across channels to avoid interference
- Delivers high reliability in challenging radio environments

Coexistence with Other Wireless Networks

- Clear Channel Assessments tests for available channels
- Blacklisting avoids frequently used channels
- Optimizes bandwidth and radio time
- Time synchronization for on-time messaging

Self-Healing Network

- Adjusts communication paths for optimal performance
- Monitors paths for degradation and repairs itself
- Finds alternate paths around obstructions
- Mesh network and multiple access points

3. Secure

WirelessHART employs robust security measures to protect the network and secure the data at all times. These measures include the latest security techniques to provide the highest levels of protection available.

Protects Valuable Information

- Robust, multi-tiered, always-on security
- Industry standard 128-bit AES encryption
- Unique encryption key for each message
- Data integrity and device authentication
- Rotate encryption keys used to join the network

Protects Wireless Network

- Channel hopping
- Adjustable transmit power levels
- Multiple levels of security keys for access
- Indication of failed access attempts
- Reports message integrity failures
- Reports authentication failures
- Safe from Wi-Fi type Internet attacks

WirelessHART – How it works

WirelessHART is a wireless mesh network communications protocol for process automation applications. It adds wireless capabilities to the HART Protocol while maintaining compatibility with existing HART devices, commands, and tools.

Each *WirelessHART* network includes three main elements:

- **Wireless field devices** connected to process or plant equipment. This device could be a device with *WirelessHART* built in or an existing installed HART-enabled device with a *WirelessHART* adapter attached to it.
- **Gateways** enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.
- **A Network Manager** is responsible for configuring the network, scheduling communications between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, host application, or process automation controller.

The network uses IEEE 802.15.4 compatible radios operating in the 2.4GHz Industrial, Scientific, and Medical radio band. The radios employ direct-sequence spread spectrum technology and channel hopping for communication security and reliability, as well as TDMA synchronized, latency-controlled communications between devices on the network. This technology has been proven in field trials and real plant installations across a broad range of process control industries.

Each device in the mesh network can serve as a router for messages from other devices. In other words, a device doesn't have to communicate directly to a gateway, but just forward its message to the next closest device. This extends the range of the network and provides redundant communication routes to increase reliability.

The **Network Manager** determines the redundant routes based on latency, efficiency and reliability. To ensure the redundant routes remain open and unobstructed, messages continuously alternate between the redundant paths. Consequently, like the Internet, if a

message is unable to reach its destination by one path, it is automatically re-routed to follow a known-good, redundant path with no loss of data.

The mesh design also makes adding or moving devices easy. As long as a device is within range of others in the network, it can communicate.

For flexibility to meet different application requirements, the WirelessHART standard supports multiple messaging modes including one-way publishing of process and control values, spontaneous notification by exception, ad-hoc request/response, and auto-segmented block transfers of large data sets. These capabilities allow communications to be tailored to application requirements thereby reducing power usage and overhead.

Components of WirelessHART technology

A **Gateway** provides the connection to the host network. *WirelessHART* and then the main host interfaces such as Modbus – Profibus – Ethernet. The Gateway also provides the network manager and security manager (these functions can also exist at the host level – however initially they will be in the gateway)

The Network manager builds and maintains the MESH network. It identifies the best paths and manages distribution of slot time access (*WirelessHART* divides each second into 10msec slots) Slot access depends upon the required process value refresh rate and other access (alarm reporting – configuration changes) The **Security manager** manages and distributes security encryption keys. It also holds the list of authorized devices to join the network.

The **Process** includes measuring devices – the HART-enabled instrumentation.

A **Repeater** is a device which routes *WirelessHART* messages but may have no process connection of its own. Its main use would be to extend the range of a *WirelessHART* network or help “go around” an existing or new obstacle (New process vessel). All instruments in a *WirelessHART* network have routing capability which simplifies planning and implementation of a wireless network.

The **Adapter** is a device which plugs into an existing HART-enabled instrument to pass the instrument data through a *WirelessHART* network to the host. The adapter could be located anywhere along the instrument 4-20mA cable; it could be battery powered or obtain its power from the 4-20Ma cable. Some adapters will be battery powered and use the same battery to power the instrument as well – in this case there will be no 4-20mA signal to the host – all process data will be reported via *WirelessHART*

A **Handheld Terminal** may come in two versions. In the first case, the handheld will be a standard HART FSK configuration unit (just add new device DDs or DOF files), just like the one used for everyday tasks such as routine maintenance and calibration checks. In the case of wireless support, the handheld is used to join a new instrument to an existing *WirelessHART* network.

In the second case the handheld has a *WirelessHART* connection to the gateway and then down to an instrument and could be used for reading PV or diagnostics.

WirelessHART Security

WirelessHART employs robust Security measures to protect the network and secure the data at all times. These measures include the latest security techniques to provide the highest levels of protection available.

Protects Valuable Information – It's Automatic

- Robust, multi-tiered, always-on security
- Industry standard 128-bit AES encryption
- Unique encryption key for each message
- Data integrity and device authentication
- Rotate encryption keys used to join the network – automatic or on-demand

Protects Wireless Network

- Channel hopping for security protection and co-existence
- Multiple levels of security keys for access
- Indication of failed access attempts – a rogue device
- Reports message integrity and authentication failures
- Safe from Wi-Fi type Internet attacks

WirelessHART technology was designed to enable secure industrial wireless sensor network communications while ensuring ease-of-use is not compromised.

Security is built in and cannot be disabled. Security is implemented with end-to-end sessions utilizing industry standard AES-128-bit encryption – approved by the National Security Agency (NSA) for top secret information. These sessions ensure that messages are enciphered such that only the final destination can decipher and utilize the payload created by a source device.

This means that no one can spy on your plant operations or inject “bad” or misleading process information.

Risk Assessment / Reduction To be a credible threat, an attacker must possess access, knowledge, and motivation. The *WirelessHART* technology Security architecture helps users address all three of these areas:

- *Minimize, control, and audit access*
- *Require high levels of technical expertise to subverted*
- *Reduce the consequences (span and duration) of any individual security breach*

Wireless Sensor Network Security can be broken down into two main categories:

- **Data Security** or Confidentiality deals with maintaining the Privacy and Integrity of the information being passed over the network.
- **Network Security** or Availability deals with maintaining the functionality of the network in the face of internal and/or external attacks (intentional or unintentional).