

**International Journal of Research Publication and Reviews** 

Journal homepage: www.ijrpr.com ISSN 2582-7421

# **Hart Communication**

# Vishala I L, Deepthi B S

Dept. of ECE, SJCIT, Chikkaballapur, India

#### ABSTRACT:

For many years, the field communication standard for process automation equipment has been a milliamp (mA) analog current signal. The milliamp current signal varies within a range of 4- 20mA in proportion to the process variable being represented. Li typical applications a signal of 4mA will correspond to the lower limit (0%) of the calibrated range and 20mA will correspond to the upper limit (100%) of the calibrated range. Virtually all installed systems use this international standard for communicating process variable information between process automation equipment. HART Field Communications Protocol extends this 4- 20mA standard to enhance communication with smart field instruments. The HART protocol was designed specifically for use with intelligent measurement and control instruments which traditionally communicate using 4-20mA analog signals. HART preserves the 4- signal and enables two way digital communications to occur without disturbing the integrity of the 4-20mA signal.

Keywords- HART Communication

## INTRODUCTION

HART stands for: Highway Addressable Remote Transducer. Field networks are not the only solution when plant operators want to use the advantages of smart field devices. The HART protocol provides many possibilities even for installations that are equipped with the conventional 4 to 20 mA technique. HART devices communicate their data over the transmission lines of the 4 to 20 mA system. This enables the field devices to be parameterized and started up in a flexible manner or to read measured and stored data (records). All these tasks require field devices based on microprocessor technology. These devices are frequently called smart devices. Introduced in 1989, this protocol has proven successful in many industrial applications and enables bidirectional communication even in hazardous environments. HART allows the use of up to two masters: the engineering console in the control room and a second device for operation.Unlike other digital communication technologies, the HART protocol maintains compatibility with existing 4-20mA systems, and in doing so, provides users with a uniquely backward compatible solution. HART Communication Protocol is wellestablished as the existing industry standard for digitally enhanced 4- 20mA field communication

#### Ph TRANSDUCER

The pH transducer is made of a sensor and an adaptor. The sensor measures an electric potential between two electrodes, the potential generated by the hydrogen ions. Since the transformation of the tension generated by the sensor in pH units is difficult, there is necessary the use of a signal adaptor. This is provided with multiple functions, including the analogousnumerical conversion, numerical calculi, generation of the outlet analogous signal and the transfer of the internal information by using the HART communication protocol. The interconnection between the two control systems is such that the surfaces can be deflected simultaneously to produce combined pitching and rolling moments. Another example of combined controls is the one applied to some light aircraft having a 'V' or 'butterfly' tail. In this case, the control surfaces operate as either a rudder or.as elevators, and for obvious reasons, they are known as ruddervators.\

## PH MEASUREMENT PRINCIPLE

The two electrodes of the sensor define a galvanic cell, the electric potential resulted being dependent on both electrodes. The ideal measurement conditions exist only when the potential of the measurement electrode depends on the variations of the pH, while the potential of the reference electrode remains constant. The tension measured may be expressed by the Nernst equation. By using the pH definition, the dependence on the pH temperature may be expressed through the relation. The temperature plays an important role concerning both the calibration and the measurement of the pH parameter. Directing the characteristic for a number of different temperatures emphasizes the fact that the lines intersect/cross in almost the same point, Fig. 1 [3]. This point is named the potential point or the izo-pH. The izo pH is usually determined after a normal calibration in two points, by realization of third calibration. The structure of the pH transducer includes an adaptor with a complex structure. Since the sensor has a differential structure, there is necessary some primary processing of the signals generated by this one. A special issue is related to the calculus of the pH value and to the automatic correction of the pH with the temperature. The volume and the complexity of the calculi have imposed the analogous-numerical conversion of the signals generated by the sensor for numerical processing of these ones. Furthermore, the adaptor has to generate signals compatible to the control

equipments, the minimum standard being the unified signal generation, one of the standards being the HART.

#### **ELECTRODE DESCRIPTION**

The measurement electrode contains a tube of glass that is permeable for the hydrogen ions. The tube is filled inside with a constant pH solution, Fig. 2. The hydrogen ions may spread inside or outside the glass tube, depending on the difference between the ions concentration in the measurement solution and the neutral solution inside the tube. The reference electrode aims at generating a stable electric environment, uninfluenced by the measurement solution pH, a potential that may be compared with the potential generated by the measurement electrode. This electrode is built of nonpermeable glass for the hydrogen ions found in the measurement solution. Building the electrode implies leakage of the internal solution or of the reference electrode in the measurement solution. The industrial electrodes are built by combining the two electrodes within one structure, Fig. 4 [6]. The industrial sensor has the measurement electrode placed inside and the reference electrode is located around the measurement electrode. This type of sensor is much easier to manipulate than two separated electrodes, the component parts of the sensor having the same properties as the separated electrodes.

## TRANSDUCER ADAPTOR

The pH sensor is supplied by the manufacturing company along with an adaptor. This adaptor fulfils several functions .The primary processing of the signals generated by the measurement sensor, the reference sensor and thermal resistance. The analogous-numerical conversion of the acquired signals. The calculus of the pH value and the correction with the temperature. The interface for the transducer calibration Displaying the pH and the temperature. Communication at DTM level is achieved by using HART or Profibus-type communication protocols. Should these protocols be lacking, communication between the respective equipment and PACT ware software instrument would not possible. The DTMs allow for the user to configurate and change the working parameters for each connected device.

# NETWORK ARCHITECTURE

On one end the WHI will be connected with any of Wireless HART wireless device and on the other side it will be connected with the HART Master. The connection between the Wireless HART devices and the WHI is through IEEE 802.15.4 as Wireless HART physical layer uses IEEE 802.15.4 wireless interface, whereas the connection between the WHI and HART Master can be any Recommended Standard (RS) discussed in IV-E. The HART Master is directly connected with slave devices that actually read process information. The HART Master can be any of the I/O system, DCS, Field controller, etc. From the Wireless HART point of view the WHI is yet another wireless device and from the HART viewpoint the WHI is a HART remote I/O system. The shows a network architecture where the WHI is used as a network integrator to connect a HART and a Wireless HART network.

Unlike tradition Wireless HART adapter that can act as both HART Master or HART slave the WHI act a as remote I/O. The WHI has no direct connection with the HART slave devices. It interacts with the slave device through the HART Master. However the WHI needs to implement Send Command to Sub-Device (Command 77) and act as a bridging device and sets Protocol Bridge Device in the Flags byte of Identity command. This is necessary to tunnel/route gateway and host application messages to the HART slave devices. When a WHI receives a message from a Wireless HART device that need to be forwarded to a HART Salve it first extracts the actual Wireless HART data i.e. the aggregated Transport layer commands, and the destination slave device address. The WHI also knows the address of the connected HART Master. Later, the WHI constitutes a HART slave device Protocol Data Unit (PDU) by embedding the Slave message inside the Master message inside the network. The WHI acts as a protocol converter that converts between HART and Wireless HART protocols. The protocol conversion occurs at the data-link layer. It shows the schematic representation of the WHI's connections with Wireless HART device and HART Master. The WHI converts the Wireless HART Network Layer PDUs to the HART data-link layer PDUs and vice versa. Both HART and Wireless HART use the same addressing schemes and only the tag length in Wireless HART is increased to 32 character, the WHI adds this tag accordingly. The WHI may provide two way accessibility i.e. the Wireless HART network can be accessed through the HART network and vice versa. However this may lead to serious security concerns when a device in an insecure HART will access the secure Wireless HART network. Section IV-E. Digital device information is communicated by encoding a digital signal, generally using a technique known as Frequency Shift Keying on the same 4-20mA wiring used for analog communications. The digital signal contains information from the device including PV, device status, diagnostics, and additional measured or calculated values, etc. Together, the two communication channels provide a complete field communications solution that is easy to design, simple to use, low cost and extremely reliable. The HART communication protocol has become a widespread solution, allowing for convenient and efficient parameterization of smart (intelligent) measuring devices. Additionally, device-specific diagnostic data can be read which provides information about the device's physical health and allow for predictive maintenance. Monitoring various device parameters is also possibility with the HART protocol

#### **MESSAGE FORMATION**

In order to send a message from a WHI to a HART slave device the HART message is wrapped inside another HART message, It shows this

wrapping. In this figure, the Slave Address Master Address To Slave To Slave Fig. 8. Routing HART PDU from WHI to HART Slave through HART Master address in the upper HART message is the Master address and the address in the embedded HART message is the actual slave address to whom the message is destined. The WHI uses HART Send Command to Sub-Device (Command 77) to tell the connected HART Master how to route the embedded message to the actual slave device.

#### JOINING AND SCHEDULING

The WHI is yet another Wireless HART wireless device and it has a Device ID and a Join Key which the WHI uses to join the Wireless HART network. After a successful join operation the WHI receives a nickname2, the Network Key to securely send messages to the neighboring devices that are one hop apart, and Session Keys to create secure sessions with the gateway and Network Manager [11]. From the Wireless HART network all messages are securely sent to the WHI that forwards them to the actual slave devices; the security between the WHI and HART Master is discussed in Section IV-E. Wireless HART network Manager and gateway respectively. The Wireless HART Network Manager assigns a nickname and a unique ID only to the WHI and not to the connected Master and slave devices. This is because the HART Master and slaves are not Wireless HART devices and hence cannot create secure session with the gateway and the Network Manager. The Send Command to Sub-Device (Command 77) allows the WHI to pass embedded HART command to a destination sub-device i.e HART Master in this case. This significantly simplifies the Network Manager's scheduling job, i.e. slot assignment, channel hopping, routing, etc.. The Network Manager only needs to schedule the WHI in the Wireless HART network (see section 9.5 in [4]) and not the HART Master and slaves. This is also true if we use adapters to connect HART slave devices with the Wireless HART network; only adapters are scheduled and not the slave devices. However, the HART devices may incur overhead in the Wireless HART network; Section VI-A discusses this overhead.

#### **CONNECTION BETWEEN WHI AND HART MASTER**

The scheduling of HART devices in the WHI is not a major issue as only one HART Master is connected with the WHI. The HART Master is responsible for scheduling the connected slave devices which is well defined in the HART protocol. The WHI maintains a queue of requests for both HART side and Wireless HART side devices to allow systematic access to networks. Wireless HART uses TDMA to ensure contention free transmission. Each time-slot is 10ms long [1]. The WHI as a Wireless HART must meet this requirement. However, the response times on the wired HART networks is slower and it is not expected that the Command 77 will complete within a 10ms time slot. Hence the WHI as an I/O system must use the delayed response mechanisms, see section 7 in [8]In a power-operated system the pilot's control is connected to the control lever only, whilethe servo-unit is directly connected to the flight control surface. Thus, in the example considered, the effort required by the pilot to move the control column is simply that needed to move the control lever and control valve piston. It does not vary with the effort required to move the control surface which, as will be noted from the diagram, is supplied solely by servo-unit hydraulic power. Since no forces are transmitted back to the pilot he has no 'feel' of the HART. I/O system, Distributed Control System(DCS), field controller, or a Field Transmission Assembly (FTA). If the Master is a remote I/O, a DCS, or a field controller the connection between the WHI and Master can be Ethernet, RS485, or even Wi-Fi (if devices support it). However, if the Master is a FTA the connection will be RS485. In this case the WHI will handle commands 0-3, 11, and 13 [15]. The WHI can be placed just near to the HART Master and wiring will not be an issue as the WHI is wirelessly connected with the Wireless HART devices. However, security is a concern here as Wireless HART is a secure network and HART network is an insecure network. If the WHI and the HART Master are placed closed to each other in a secure physical environment, it will be hard to eavesdrop the wired communication link. Also, as there are no intermediate devices between WHI and HART Master it is hard to compromise the integrity of the message by a man-in-the-middle attack. However, the authentication of connected HART Master to the WHI and vice versa may be needed. Both WHI and HART Master are wired devices and resource scarcity is not really an issue. We propose the use of Public Key Infrastructure (PKI) based solution to secure this link. The Wireless HART Security Manager is a trusted entity in the Wireless HART network that can be used to build a PKI.

Earlier designed and implemented a Security Manager for the Wireless HART networks [14]. Our Security Manager, besides providing security services to the Wireless HART wireless devices, is used to secure the communication between the Wireless HART wired entities such as between the gateway and the Network Manager, gateway and host application, and Network Manager and Security Manager. To secure WHIHART Master links, our Security Manager is able to generate and provide private keys and signed X.509 certificates to both WHI and HART Master. Before the actual communication, the WHI and HART Master can authenticate each other using these security credential and PKI [16]. This solution can be used to provide Confidentiality and Integrity, if needed.

#### GATEWAY AND THE ADAPTER

The HART is presented different ways to connect HART and Wireless HART devices/networks. The choice of the specific approach depends on user needs and the underlying HART architecture, e.g. adapter is the most appropriate choice when we need to connect a single HART device with a Wireless HART network. In this section we compare WHI versus gateway and WHI versus adapter based solution to integrate HART and Wireless HART networks. the gateway may also connect a Wireless HART network with other automation networks such as the Fieldbus [17] or ISA 100.11a [18]. Due to the proximity of the gateway it is sometimes simply not feasible to connect the gateway with the HART network using physical wiring. In real deployments HART wiring is already a mess. However, if the HART network is connected with the Ethernet using a HART modem and it is

feasible to connect the gateway with the same PC where the HART modem is plugged in the gateway may be a better alternative to connect the two networks. Unlike a gateway, the WHI is a wireless and portable device and the change of the physical location will not require additional wiring as the WHI has only one physical link i.e. with the HART Master. In an automation plants there are usually more than one HART networks. We may use multiple WHIs to connect more than one HART network with the Wireless HART. Since there is only one gateway in a Wireless HART network [8] the gateway based solution may not be used to connect multiple HART networks with the Wireless HART network; this is a major limitation of the gateway based solution. Security is a distinctive feature of Wireless HART. A gateway based integration is less secure as the messages in the HART backbone flow as plain text all the way to the Wireless HART networks, unless the gateway is directly connected to the HART Master which is usually not feasible. The physical position of the gateway affects security: the closer the gateway to the HART Master the soonerloop. The flight test program confirmed the quality of the validation process by achieving 50 flights without a known undetected failure and with no false alarms. F-8 Digital Fly-ByWire (left) and F-8 Supercritical Wing in flight. These two aircraft fundamentally changed the nature of aircraft design. The F-8 DFBW pioneered digital flight controls and led to such computer-controlled aircraft as the F-117A, X-29, and X-31. Airliners such as the Boeing 777 and Airbus A320 also use digital fly-by-wire systems. The other aircraft is a highly modified F8A fitted with a supercritical wing. The F-8 Digital Fly-By-Wire (DFBW) flight research project validated the principal concepts of all-electric flight control systems now used on nearly all modern high-performance aircraft and on military and civilian transports. The first flight of the 13-year project was on May 25, 1972, with research pilot Gary E. Krier at the controls of a modified F-8C Crusader that served as the testbed for the fly-by-wire technologies. The project was a joint effort between the NASA Flight Research Center, Edwards, California, now the Dryden Flight Research Center and Langley Research Center. It included a total of 211 flights. The last flight was December 16, 1985, with Dryden research pilot Ed Schneider at the controls. The F-8 DFBW system was the forerunner of current fly-bywire systems used in the space shuttles and on today's military and civil aircraft to make them safer, more maneuverable, and more efficient. Electronic fly-by-wire systems replaced older hydraulic control systems, freeing designers to design aircraft with reduced in-flight stability. Fly-by-wire systems are safer because of their redundancies. They are more maneuverable because computers can command more frequent adjustments than a human pilot can. For the NASA Dryden Flight Research Center is flight testing a triply redundant digital flyby-wire (DFBW) control system installed in an F-8 aircraft. The full-time, full-authority system performs three-axis flight control computations, including stability and command augmentation, autopilot functions, failure detection and isolation, and self-test functions. Advanced control law experiments include an active flap mode for ride smoothing and maneuver drag reduction. This paper discusses research being conducted on computer synchronization, fault detection, fault isolation, and recovery from transient faults

# LITERATURE SURVEY

Ake Norberg et al.[1] discussed relevant to the study of monocopter stability is the stability of maple seeds in autorotation. His qualitative directional stability analysis was expanded into a quantitative analysis for monocopters. McCutchen et al.[2] discussed a qualitative description of monocopter stability, and a brief description of how control of the vehicle could be effected using an under-slung fuselage. McCutchen makes the leap to say that future technology could make free-flying controlled monocopters possible. Andreas Kellas et al.[3] discusses the implementation of a rudder-control scheme for an autorotating vehicle similar to a maple seed. While Kellas does not clearly demonstrate control in flight tests, his work shares the challenge of detecting the orientation of an all-rotating vehicle. Whitecomb et al.[4] discusses the computer-controlled flight systems pioneered by the F8 DFBW created a revolution in aircraft design. The F-117A, X-29, X-31, and many other aircraft have relied on computers to make them flyable. David et al.[5] discusses the envelope protection systems and aviation free space technology. The F-8 DFBW simulator was used in the development, testing, and validation of an all digital flight-control system installed in the F-8 aircraft that replaced the normal mechanical/hydraulic controls. Many military and commercial aircraft have digital flight control systems based on the technologies developed at NASA Dryden. J.Tom et al.[6] discusses the story of flight control system Dryden Flight Research Center engineers, in partnership with industry leaders such as Cambridge, Massachusetts-based Draper Laboratory, demonstrated that digital computers could be used to fly aircraft. Digital fly-by-wire systems have since been incorporated into large airliners, military jets, revolutionary new aircraft, and even cars and submarines. Boulton Paul et al.[7] discusses the Air craft douty packages system of aircraft control. The forms of representation of the flight envelope and the process by which identified parameters are used to modify the gain schedule. It contains data taken during piloted real-time 6 degree-of-freedom simulations that were used to develop and evaluate the system.

#### ADAPTER BASED SOLUTIONS

A single Wireless HART adapter connects only one HART device to the Wireless HART network if the underlaying HART network is point-topoint current looped. A single adapter can connect multiple devices with the Wireless HART network if the HART network is multidrop current looped. In point-topoint HART network, connecting multiple HART devices is cumbersome and does not scale since we need an adapter for each device. Theoretically, up to to 275,000,000,000 slave devices can be connected to a current loop but normally not more than 15 devices are connected to a multi-drop current loop in order to keep noise in transmissions down [3]. Connecting the (point-to-point) HART network with 15 devices to a Wireless HART network requires 15 adapters. Hence an adapter is not a feasible solution to connect HART and Wireless HART networks. The key advantage of the WHI over adapterbased solutions is scalability in that the number of additional devices in the Wireless HART network is lower using the WHI-based solution .The choice of the specific approach depends on user needs and the underlying HART architecture, e.g. adapter is the most appropriate choice when we need to connect a single HART device with a Wireless HART network. In this section we compare WHI versus gateway and WHI versus adapter based solution to integrate HART. The Wireless HART standard is in its inception stage and the architecture of Wireless HART Network Manager is still not clear in the standard. Also, we have no open gateway and Network Manager to test our solution. Therefore, we cannot conduct experiments with real Wireless HART networks. However, we theoretically evaluate our WHI, the gateway, and the adapters based solutions using network parameters such as bandwidth, computation, security, reliability. There is only one gateway in the Wireless HART network. The use of a gateway as an integrator may be a suitable choice in some scenarios but the proximity and placement of the gateway in the automation plant may not allow wired connections with multiple HART networks. In many deployments, the wiring of the HART network is already a mess. Moreover, the gateway based integration is not secure as the messages in the HART network travel all the way to the gateway without security. We present a novel, comparatively secure, and scalable solution to connect HART and Wireless HART network. In Section V we will analyze the gateway based integration and our solution. In the next section we present our solution.

Altitude information essential for vertical guidance to touchdown is always provided by signals from a radio altimeter which becomes effective as soon as the aircraft's altitude is within the altimeter's operating range. When the aircraft has descended to 1,500 feet radio altitude, the localizer and glide slope beams are captured, and the armed 'off-line' control channels are then automatically engaged. The localizer and glide slope beam signals control the aircraft about the roll and pitch axes so that any deviations are automatically corrected to maintain alignment with the run way. At the same time, the auto land status annunciator displays 'LAND 2' or 'LAND 3', depending upon the number of channels 'voted into operation' for landing the aircraft, and computerized control of flare is also armed. At a radio altitude of 330 feet, the. aircraft's horizontal stabilizer is automatically repositioned to begin trimming the aircraft to a nose-up attitude. The elevators are also deflected to counter the trim and to provide subsequent pitch control in the trimmed attitude. When an altitude is reached at which the landing gear is 45 feet above the ground referred to as gear altitude the flare mode is automatically engaged. The gear altitude calculation, which is pre-programmed into the computer, is based upon radio altitude, pitch attitude, and the known distance between the landing gear, the fuselage and the radio altimeter antenna. The flare mode takes over pitch attitude control from the glide slope, and generates a pitch command to bring the aircraft onto a 2 feet/second descent path. At the same time, a 'throttle retard' command signal is supplied to the auto throttle system to reduce engine thrust to the limits compatible with the flare path. Prior to touchdown, and about 5 feet gear altitude, the flare mode is disengaged and there is transition to the touchdown and roll-out mode. At about 1 foot gear altitude, the pitch attitude of the aircraft is decreased to 2°, and at touchdown, a command signal is supplied to the elevators to lower the aircraft's nose and so bring the nose landing gear wheels in contact with the runway and hold them there during the rollout. When reverse thrust is applied, the auto throttle system is automatically disengaged. The AFCS remains in control until disengaged by the flight crew.

#### NETWORK OVERHEAD

Connecting HART network with the Wireless HART network through WHI apparently inserts large overhead in the Wireless HART network and may prone to the network congestion, collision, interference, etc. However, this is actually not the case as Wireless HART offers time slotting (using TDMA scheduling) and channel hopping (FHSS). Although the WHI may utilize more network resources (bandwidth, time slots, etc) there will probably be very low interference and collisions (as Wireless HART standard claims) as each message will be sent in specific time slot and on particular channel. Wireless HART uses the 2.4 GHz frequency band. It shared this band with ZigBee, Bluetooth, ISA 100.11a, etc which makes it prone to interference. All messages in the Wireless HART network flow through gateway, i.e two devices must have sessions with the gateway to communicate with each other; Handheld device creates direct peer-to-peer sessions. In the WHI based solution HART messages traverse the Wireless HART twice i.e. from WHI to gateway and from gateway to the destination device. On the other hand, the gateway provides a more Wireless HART friendly solution as HART messages will only travel from the gateway to the destination devices. The bandwidth requirements in the Wireless HART network will be high in adapters and WHI based solutions, whereas bandwidth requirements in the HART backbone will be high in HART. The Wireless HART standard is in its inception stage and the architecture of Wireless HART Network Manager is still not clear in the standard. Also, we have no open gateway and Network Manager to test our solution. Therefore, we cannot conduct experiments with real Wireless HART networks. However, we theoretically evaluate our WHI, the gateway, and the adapters based solutions using network parameters such as bandwidth, computation, security, reliability, scalability, etc. The WHI can be placed just near to the HART Master and wiring will not be an issue as the WHI is wirelessly connected with the Wireless HART devices. However, security is a concern here as Wireless HART is a secure network and HART network is an insecure network. If the WHI and the HART Master are placed closed to each other in a secure physical environment, it will be hard to eavesdrop the wired communication link. Also, as there are no intermediate devices between WHI and HART Master it is hard to compromise the integrity of the message by a man-in-the-middle attack. However, the authentication of connected HART Master to the WHI and vice versa may be needed. Both WHI and HART Master are wired devices and resource scarcity is not really an issue. We propose the use of Public Key Infrastructure (PKI) based solution to secure this link. The Wireless HART Security Manager is a trusted entity in the Wireless HART network that can be used to build a PKI.

#### BANDWIDTH

The Wireless HART operates at 250 kb/s, HART operates at 1200 bits/s, and the HART backbone is connected through Ethernet that provides bandwidth in MBs. The high bandwidth in the HART backbone allows messages to reach the gateway faster than through the Wireless HART network. However, the gateway is a central hub and is physically connected to many other devices (Network Manager, APs, Host applications, etc. ) and may be with networks such as ISA100.11a [18], Fieldbus [17], etc. The gateway maintains a queue of requests for all these wireless and wired devices and networks. The gateway and the WHI may also need to maintain a queue of request for the HART network. Having multiple connections with other devices and networks the queuing time in the gateway based design increases and the overall latency in gateway based integration may become higher than the WHI based integration. The 'MCP SPD' is annunciated to indicate to the flight crew that pressing the switch will cause the auto throttle system to revert to 'ARM'. In the event of speed mode operation with an engine 'out', the throttles advance together to maintain airspeed, and NI speed equalization is replaced by thrust lever equalization. Approach gain of the auto throttle system is determined either by glide slope capture or by radio

altitude, and flap position. Approach gain provides high gain setting for more precise speed control, and reduced throttle motion during changes of flap position. During an approach in turbulent conditions, the gain tends to cause the system to be high on speed. The degree of over speed depends on the magnitude and frequency of the turbulence. During the landing flare manoeuvre, the retard rate of thrust reduction is adjusted so that throttle angle is reduced to idle in 6 s. Retard occurs at 27 feet of radio altitude during an automatic or manual landing. If it is not initiated by radio altitude, it can also occur 1.5 s after an automatic communication.

# CONCLUSION

Using Gateway, adapters, or WHIs can be used to interconnect HART and Wireless HART networks. However the best choice depends to a large extent on user needs and the properties of the deployed HART network. Adapters are appropriate to connect multi-drop HART network devices with Wireless HART networks. When there is only one point-to-point HART network in the automation plant and it is feasible to securely and directly connect the gateway with the HART Master then the gateway based interconnection is the appropriate choice. Usually there are multiple HART networks in an automation plant and because of having only one gateway it is not feasible to directly connect the gateway with all the HART Masters since wiring will be cumbersome.

## REFERENCES

- 1. Gunther CW, Verbeek E. XES Standard Definition, Eindhoven University of Technology, vol. 6, pp. 2, 2021.
- 2. Hughes D. Documentation for Lars. Mime Consulting. 2013. Available at: Accessed December 10, vol. 18, pp. 302, 2013.
- 3. Jamari P, Improving the Performance of Proxy Server by Using Data Mining Technique. World Academy Of Science, Engineering and Technology, vol. 8, pp. 53, 2013.
- 4. Kowhai R, Mining E-Commerce Data: The Good, the Bad, and the Ugly, KDD 2001 Industrial Track, vol. 7, pp. 243, 2001.
- 5. Liu B. Web Data Mining. 2nded. Springer Berlin Heidelberg; 2011. ISBN: 9783642194597.
- 6. Perner P, Fiss G, Intelligent E-Marketing with Web Mining, Personalization and User-adapted Interfaces. Data Mining in ECommerce, Medicine, and Knowledge Management, vol. 32, pp. 342, 2002.
- Poggi N, Muthusamy V, Carrera D, Khalaf R. Business Process Mining from E-commerce Web Logs. Springer Berlin Heidelberg, vol. 3, pp. 22, 2013.
- 8. Srivastava J, Cooley R, Deshpande M, Tan P-N. Web Usage Mining: Discovery and Applications of usage Patterns from Web Data. SIGKDD Explorations, vol. 22, pp. 88, 2000.
- 9. Monitoring web traffic source effectiveness with Google Analytics: An experiment with time series, vol. 61, no. 5, pp. 474-482.
- 10. Phippen A, Sheppard L & Furnell S, A practical evaluation of Web analytics. Internet Research, vol. 14(4), pp. 284-293.
- 11. Nakatani, K., & Chuang, T. T, A web analytics tool selection method: an analytical hierarchy process approach. Internet Research, vol. 21(2), pp. 171-186, 2011.
- 12. Erturk, E, A case study in open source software security and privacy: android adware, Internet Security (WorldCIS), 2012 World Congress on, pp. 189-191, 2012.
- 13. Kaushik, A. Web analytics: An hour a day. Chichester: Wiley; 2007.