MOORE INDUSTRIES WORLDWIDE

Bridging the Gap between HART Devices and IIoT, the Industrial Internet of Things

Overview

Over the last couple of decades, the introduction of industrial Ethernet and wireless networks in process manufacturing plants and automation facilities has meant that data exchange within a facility and even throughout global corporate networks is becoming commonplace. The separate information hierarchy levels, outlined in the ISA 95 model, related to process data exchange within a manufacturing facility, have started to coalesce. In prior years, data and information that needed to be exchanged between the lowest plant floor levels 0-2 and the upper ERP (Enterprise Resource Planning) level 4 required expensive MES (Manufacturing Execution Systems) products or custom coding; and oftentimes both (See Figure 1). This free flow of information has introduced a new set of ubiquitous terms, standards and phrases such as IIoT (Industrial Internet of Things), Smart Factory, Cloud Automation and Industry 4.0.

This white paper will outline how the flow of process and diagnostics data from smart HART digital field instruments can now be shared with mid and higher level control, asset management and data information systems without having to upgrade expensive process control interface equipment. Additionally, features and considerations of devices that enable this sharing of data will be reviewed and suggested.

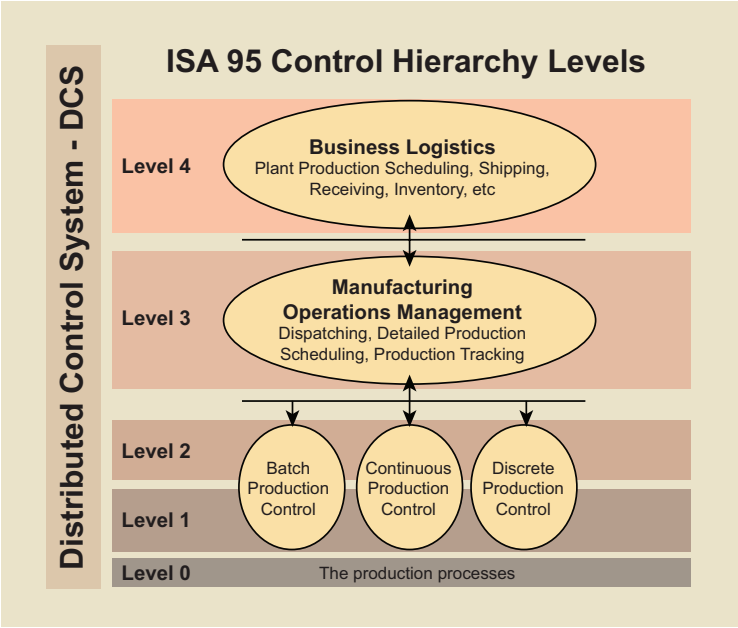


Figure 1. *ISA 95 Model Showing Control and Information Levels*

Plant of the Future

The typical process control model that involves decision making for the process at the local or centralized level by PLCs (Programmable Logic Controller) or BPCS (Basic Process Control System) is quickly changing. These systems installed yesteryear were never intended to deal with or even realize the amount of data they would have access to in the near future. There are certainly newer ERP, MES and asset management systems that collect some of this data now, but the more critical challenge that local manufacturing facilities face is manpower. Because streamlining of costs and overheads has left many manufacturing facilities with just enough personnel to keep the plant running, facilities no longer have the extra time, personnel and resources required to analyze data. For this reason we are seeing third party companies, and even some of the larger process control vendors, offer leasing or annual agreements that involve collecting, storing, and analyzing all sorts of process data. This data is part of a larger predictive analytics strategy that can not only forewarn operators of impending problems to come, but is also being used to optimize the process itself. This type of cloud automation looks to gather as much data as possible to reduce operating expenditures and future capital expenditures for future plant builds. So the challenge remains: how do existing and new manufacturing facilities find a cost effective way to get critical plant floor data up to higher level information systems? The answer is to take advantage of the digital HART data you already have installed but either didn't know it was there or couldn't afford the equipment upgrades to gain access to it.

HART Protocol's Persistence

The process industry has had no lack of digital instruments and protocols introduced to market over the last thirty years, each promising new and improved methods of gathering and sharing process variables and diagnostics via digital communication links. However, there is only one smart instrument communication protocol that has outlasted and outsold all of these alternative options: HART, and the devices that use it. With over 40 million installed HART devices worldwide, HART is not only here to stay but unlike other protocols, it also continues to get updated revisions that continually enhance data exchange capacity, speed, number of devices on a network, support over Ethernet, and wireless capability. There is no other protocol that has the massive installed base, is open to all vendors, has proven worldwide end user support, and continues to get updates and unilateral support from nearly all mainstream device manufacturers. For these reasons, HART will continue to retain its leadership role, enabling end users to have unfettered access to process and diagnostic data that can be shared with all areas of the new Smart Factory that supports IIoT endeavors.

HART Primer

With over 40 million HART instruments installed worldwide, one might conclude that everyone understands HART protocol and what data is available from HART smart devices. Unfortunately, that conclusion is too often false. Even though HART has been around since the early '80s, end users are often surprised when they realize the amount of data they actually have access to. The following paragraphs briefly highlight what data is available from HART smart devices and how to gain access to that data (for a more in depth and complete primer on HART you can visit the FieldComm Group's website at www.fieldcommgroup.org).

HART enabled devices superimpose a digital signal upon their 4-20mA process signal. The HART digital signal often contains additional process measurements and other variables that may include instrument status, diagnostic data, alarms, calibration values and alert messages.

Many HART field transmitters are hard at work measuring process parameters, and producing a 4-20mA signal that is being used for process control by a BPCS, PLC or some other control system. In many cases, HART instruments were installed simply because they could be configured and diagnosed easily with a HART handheld

communicator (HHC). There are several reasons that the rest of the HART data often goes unused. One of them is the prohibitive cost of installing a plant wide HART monitoring system and lack of familiarity with alternatives.

A simple and cost-effective solution for gathering HART information is to use a HART interface device. These HART interface devices make acquiring HART data a fairly simple proposition. This HART data can then be made available to the control system, asset manager or plant Ethernet backbone where it can then be shared with higher level systems or corporate WANs (Wide Area Network) See Figure 2.

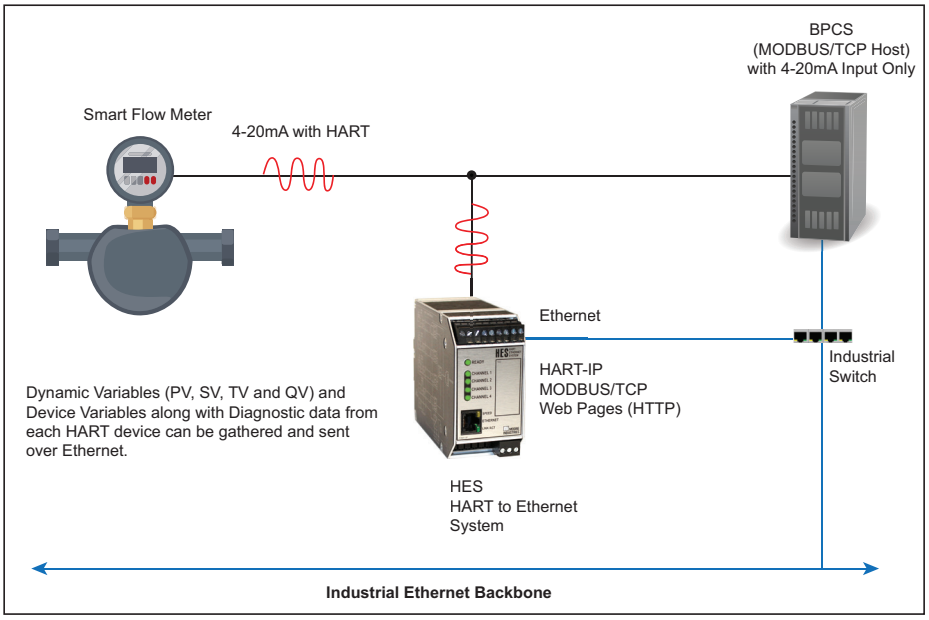


Figure 2. *A HART interface device like the HES HART to Ethernet Gateway connects to the 4-20mA process signal and extracts HART process and diagnostic variables and makes them accessible via Ethernet.*

The data gathered from smart HART interfaces or HART enabled hosts uses specifically defined universal and custom commands outlined within the HART specification. The HART specification has also had updates to the protocol, referred to as revisions, which have additional capabilities. Most HART devices operating in the field today utilize revision 5, 6 or 7. For the sake of this whitepaper we will limit the discussion to three universal commands routinely used with revisions 5, 6 and 7 to gather process and diagnostic data from field devices. Those three commands are command 3, 9 and 48.

HART Revisions and Compliance

HART field devices are compliant to a certain HART revision. Most field devices released within the last twenty years support HART revision 5, 6 or 7. Each new revision of HART offers different features and capabilities, but all field devices – regardless of revision – still support backwards compatibility with HART hosts and handheld communicators. It is important to note that earlier revisions of the HART specification may not support the full features of the latest HART commands that were enhanced or released after a device's release to market. For this reason it is important to verify what revision of HART the field device contains to ensure that the HART interface device is using the appropriate commands and receiving the expected results.

HART Dynamic and Device Variables

HART devices can provide a lot of additional data to the primary variable which is read on the 4-20mA loop. In addition to diagnostic and status bits and bytes, there are two types of HART variables that you can retrieve from HART devices: Dynamic Variables and Device Variables.

All of these HART Variables support IEEE 754 Floating Point values and are retrieved by HART hosts or interface devices (commonly referred to as gateways or multiplexers) from the field device by utilizing HART Command 3 or Command 9.

Dynamic Variables consist of the Primary Variable (PV), Secondary Variable (SV), Tertiary Variable (TV) and Quaternary Variable (QV). These variables are most often obtained from field devices using HART Command 3. However the HART specification also makes them available in later revisions as Device Variables (see below) so they could be retrieved using Command 9 too.

Device Variables may also be used in more sophisticated or multi-variable field devices to provide additional process, diagnostic or status related information. Device Variables are only available in HART 6 and 7 revision field devices and are read using HART Command 9. Each field device can define **up to** 240 Device Variables (HART 7) numbered consecutively from 0 to 239. The Device Variable Codes (HART memory map location identifier) are unique to each field device and may be defined in the operation manual or obtained from the manufacturer. In addition, the following Device Variable Codes are defined in the HART specification:

242	(Optional) Battery Voltage
243	(Optional) Battery life
244	Percent Range
245	Loop Current
246	Primary Variable (PV)
247	Secondary Variable (SV)
248	Tertiary Variable (TV)
249	Quaternary Variable (QV)

Note: On some HART field devices the Dynamic Variables - PV, SV, TV and QV, can be assigned and represented as any of the Device Variables.

HART Hosts and Revisions

Most HART hosts and interface devices can be configured as a Primary or Secondary HART host and can poll between 16 and 64 field devices (dependent on revision). Since HART Commands 3, 9 and 48 that are used for the reading of Dynamic Variables, Device Variables, and Additional Status (respectively) are Universal Commands, most hosts and interface devices support them. The HART revision of the field device will determine how it supports these Commands. This brief summary of the three HART revisions outlines which commands each one supports:

HART 5 Devices support Command 3 only.
Using Command 3, the host or interface device will read the Dynamic Variables, i.e. PV, SV, TV, QV and loop current from the field device.

HART 6 Devices support Command 3 and Command 9.
Using Command 3, the host or interfacing device will read the Dynamic Variables and loop current from the field device.

Using Command 9, the host or interfacing device can read up to four Device Variables from the field device. To use Command 9, the number of Device Variables and each Device Variable Code from the specific field device need to be specified.

HART 7 Devices support Command 3 and Command 9.
Using Command 3, the host or interfacing device will read the Dynamic Variables and loop current from the field device.

Using Command 9, the host or interfacing device can read up to eight Device Variables from the field device. To use Command 9, the number of Device Variables and each

Device Variable Code from the specific field device need to be specified.

All HART revisions support the Additional Status Command 48. HART protocol allows the manufacturer to report as many as 25 bytes of diagnostic data from each HART field device. This plays a key role in performing the overall health and status of field devices.

For multivariable and more complex HART field devices, where data is required from more than eight Device Variables, the field device can be polled multiple times by a HART host or interfacing device with each poll specifying up to eight unique Device Variables. For example, if you wanted Device Variables 2-25 from a specific field device, you could configure the host or interfacing device to poll that same field device using HART Command 9 three times specifying eight unique Device Variables with their respective Device Variable Codes in each poll.

HART Interface Options

There are several ways to interface with HART smart field devices in order to acquire the digital process and diagnostic information. They vary from HART enabled 4-20mA input cards, HART multiplexer (Mux) systems, slide-in PLC gateway cards, custom coded software interfaces for asset management and MES/ERP systems and standalone gateways that typically convert the HART data to some other proprietary or open industry format. Many PLC and BPCS cards that are installed in legacy systems don't have the capability to read the HART data that is superimposed on the 4-20mA signal. However, each vendor usually has an alternative card that is more expensive or offers a full upgrade path for the CPU/Controller and input cards that read HART.

HART multiplexers are common and typically their interface is a custom RS-422, RS-485 or RS-232 serial connection and is custom configured for a particular vendor's hardware interface, asset management system or control system. Some PLC and BPCS companies offer slide-in chassis type gateway cards that read the HART data and offer a proprietary backend communication connection to the system. Usually each of these options is quite costly and therefore often avoided. The most expensive but also most specific HART interface to have is one written by a programmer which can then be customized to exact user and hardware specifications.

Lastly are standalone HART gateways that most often provide the most economical pathway to extracting HART data from field devices, making the data readily available to higher level systems. These products usually offer one to four channels or ports that allow several HART devices to be multidropped for maximum data concentration (See Figure 3).

Employing the Extracted HART Data

Once HART data is extracted from field devices it is essential that the information is made available in an open and easy-to-interface manner. Now that Ethernet backbones (often further propagated by fiber and wireless modems for longer distances) have become the standard for in-plant communication links, it seems only reasonable that any interface device that gathers and holds enormous amounts of data should include an Ethernet port. Likewise, these same devices should support open protocols that run seamlessly over Ethernet networks.

At a minimum, Ethernet devices should offer the viewing of its collected HART process and diagnostic data via web pages supported by any PC, tablet or mobile device. For users, viewing webpages with an enormous amount of data can be overwhelming. Efforts should be made by device vendors to lay the information out in a table format

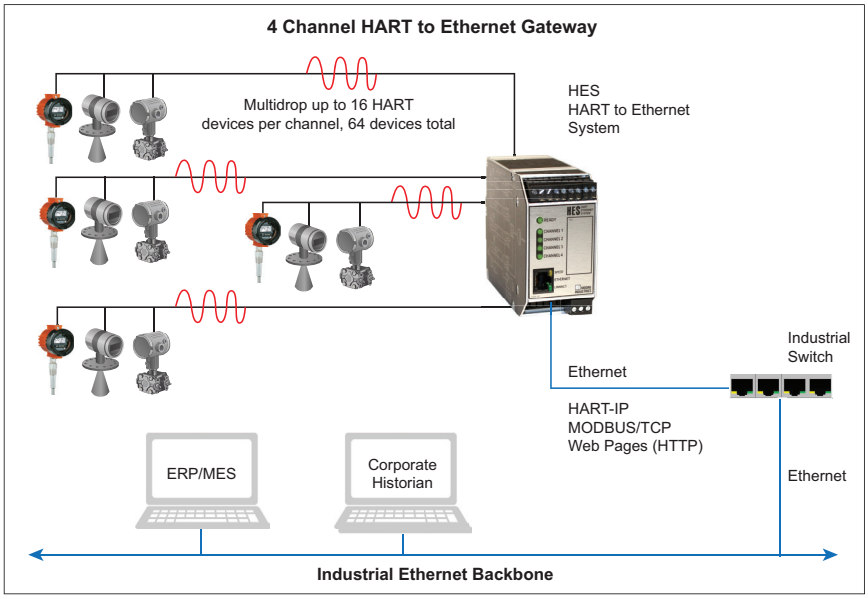


Figure 3. *HART to Ethernet Gateways offer a quick and economical way of sharing critical HART data with higher level systems*

with easy-to-understand headers and address locations (for other supported protocols) so that additional hosts can be configured more easily (See Figure 4).

Figure 4. *Web servers should display extracted HART data on web pages in easy to read tables with optional addressing for other protocols (MODBUS shown here)*

HES: HART Ethernet System

Field Device HART Data

System Summary			
Register Name	**MB Reg**	**Value**	**Status Messages**
System Overall	9501	0x0000	No status bits set
System Status Summary	9502	0x0008	(3) IO Channel Warning, see IO Channel Status Registers
Ch1 Consolidated Status	9566	0x0000	No status bits set
Ch2 Consolidated Status	9598	0x0010	(4) One or more Devices have Device Malfunction Bit Set
Ch3 Consolidated Status	9630	0x0010	(4) One or more Devices have Device Malfunction Bit Set
Ch4 Consolidated Status	9662	0x0000	No status bits set

Channel 1								
Device	**1st DV/PV Units (MBReg)**	**2nd DV/SV Units (MBReg)**	**3rd DV/TV Units (MBReg)**	**4th DV/QV Units (MBReg)**	**5th DV Units (MBReg)**	**6th DV Units (MBReg)**	**7th DV Units (MBReg)**	**8th DV Units (MBReg)**
Channel 1, Device 1 Addr: 0, CMD3 Tag: STZ001	98.235 DEG C (1)	25.346 DEG C (129)	68.236 DEG C (257)	94.325 DEG C (385)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 1, Device 2 Addr: 1, CMD3 Tag: STZ002	155.680 DEG F (3)	72.546 DEG F (131)	136.876 DEG F (259)	435.231 DEG F (387)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 1, Devices 3 to 16 are not polled.								

Channel 2								
Device	**1st DV/PV Units (MBReg)**	**2nd DV/SV Units (MBReg)**	**3rd DV/TV Units (MBReg)**	**4th DV/QV Units (MBReg)**	**5th DV Units (MBReg)**	**6th DV Units (MBReg)**	**7th DV Units (MBReg)**	**8th DV Units (MBReg)**
Channel 2, Device 1 Addr: 0, CMD3 Tag: THZ3001	89.236 DEG R (33)	285.321 DEG R (161)	88.324 DEG R (289)	352.126 DEG R (417)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 2, Device 2 Addr: 1, CMD3 Tag: THZ3002	132.453 KELVN (35)	1234.660 KELVN (163)	453.230 KELVN (291)	689.124 KELVN (419)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 2, Devices 3 to 16 are not polled.								

Employing this HART data for process monitoring, control, predictive maintenance, and process optimization requires that open and vendor neutral industrial protocols be supported . Doing so allows the HART device data to freely flow to most any control, SCADA and monitoring system from any vendor. Now that HART supports Ethernet with HART-IP, it only seems logical that any device supporting the HART protocol with an Ethernet port would support HART-IP (See Figure 5). HART-IP devices typically allow for any HART field device data to be mapped to a number of Device Variable locations for reading by a HART-IP host.

One of the most installed and supported industrial Ethernet protocols is MODBUS/TCP. MODBUS/TCP takes MODBUS data packets and wraps them in a TCP header utilizing IP addressing. This makes implementation by both host computer and field device manufacturers quick and abundant due to MODBUS' popularity and royalty free implementation (See Figure 6).

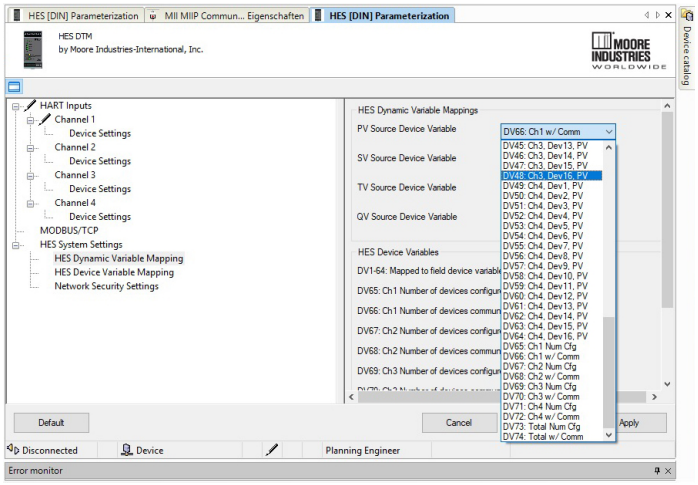


Figure 5. *HART Gateways supporting HART-IP typically allow freeform mapping of HART field device data*

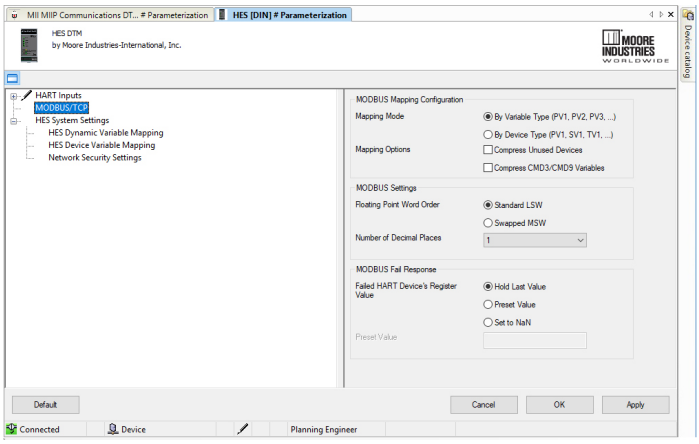


Figure 6. *HART to Ethernet Gateways should support open industrial Ethernet protocols like MODBUS/TCP*

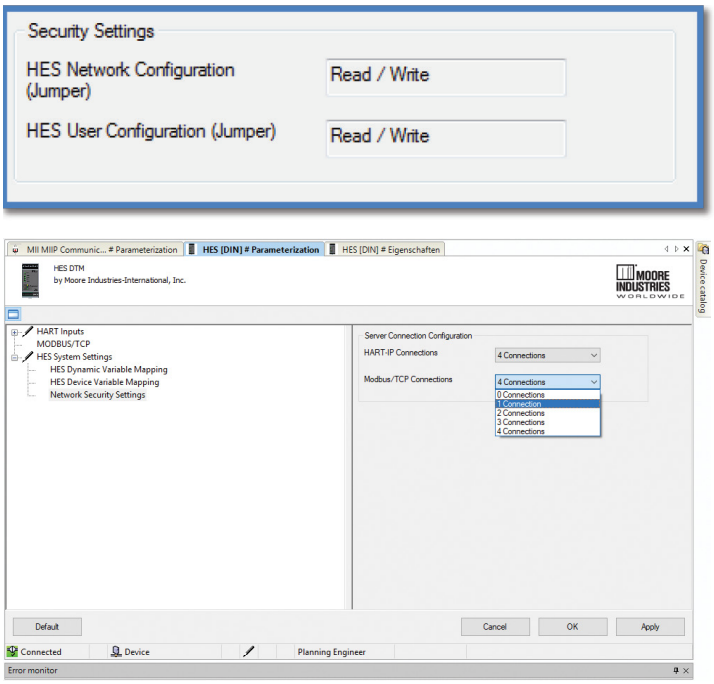
Cybersecurity Considerations

IIoT, cloud storage, big data and a host of other interconnecting methods and strategies has led to no shortage of production and efficiency increases. Unfortunately, these have not been nor do they continue to be realized without a cost and threat from cybersecurity issues. For these reasons it is more important than ever that Ethernet-based devices include safeguards within their products to ensure that network bandwidth is protected, viruses or malware cannot be loaded, unwanted access is not granted, unauthorized reconfiguration of device is not allowed, and unauthorized writes to memory locations are not accepted by the device. In addition, physical security of such devices must be restricted to authorized personnel only and process values should be read only – unless the device is required to perform control. Post installation considerations should also be taken to assist onsite protection of site data and property. At a minimum, a two layer protection scheme should be put in place for any Ethernet enabled device that includes software and physical hardware restricted access (See figure 7).

Configuration of IIoT Devices

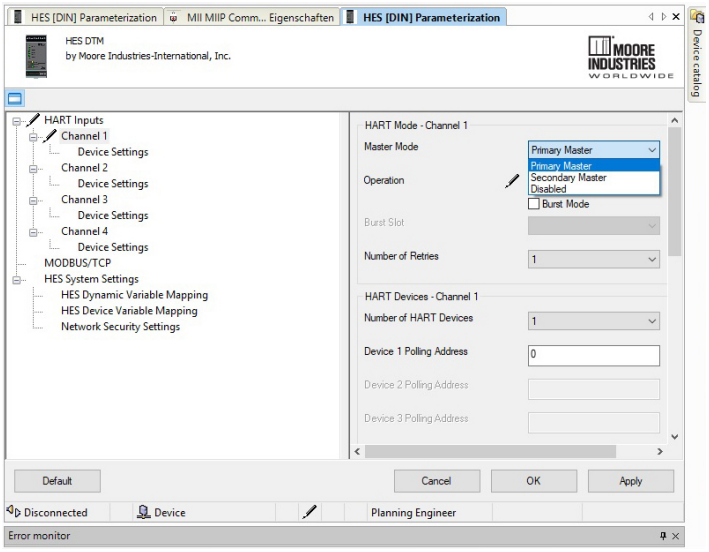
For many years, end users have had to deal with custom and proprietary configuration packages from vendors for advanced capability devices. This typically leads to several custom software packages that users have to learn, get IT support and permission for and become familiar with. Most IIoT capable devices are not straight forward field instruments and therefore small handheld configurators are not convenient for setup

Figure 7. *The HES HART to Ethernet Gateway restricts unauthorized access with a hardware solderless jumpers and software communication socket restrictions*



and configuration. In fact, many HART protocol gateways often require complex database mapping and programming software. When sourcing or specifying an IIoT device, investigate what the programming interface will be. There are several open standards and software packages that vendors have access to that prevent the need for custom and sometimes even expensive programming software utilities (See Figure 8).

Figure 8. *Look for devices that support open industry standards like FDT/DTM technology for programming, so free software like PACTware™ can be used*



Taking critical plant floor data from smart HART field devices and sharing it with higher level control and information systems within a manufacturing facility and further, no longer has to be difficult or expensive. With the acceptance of industrial Ethernet backbones and wireless networks, IIoT HART interface devices like the HES with built-in security measures, open industry protocols and ease of programming provides a quick and seamless way to share process data with the entire corporate infrastructure.

MOORE INDUSTRIES
United States • info@miinet.com
Tel: (818) 894-7111 • FAX: (818) 891-2816
Australia • sales@mooreind.com.au
Tel: (02)8536-7200 • FAX: (02) 9525-7296
BeNeLux • info@mooreind.eu
Tel: 03/448.10.18 • FAX: 03/440.17.97
China • sales@mooreind.sh.cn
Tel: 86-21-62491499 • FAX: 86-21-62490635
United Kingdom • sales@mooreind.com
Tel: 01293 514488 • FAX: 01293 536852