Bridging the gap between HART devices and IIoT

By Tina Todd, director of engineering, Moore Industries-International, Inc.

Over the last couple of decades there has been a rapid growth of industrial Ethernet and wireless networks in process manufacturing plants and automation facilities. This has resulted in data exchange within a facility, and even throughout global corporate networks, 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 article outlines how the flow of process and diagnostics data from smart HART digital field instruments can easily 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.

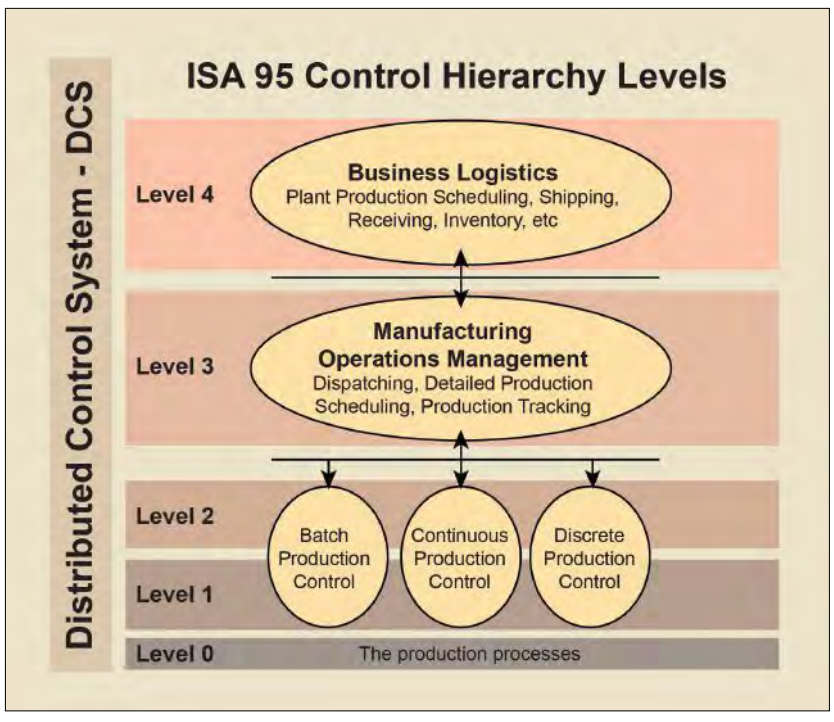


Figure 1. ISA 95 Model showing control and information levels.

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 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. Streamlining of costs and overheads has left many manufacturing facilities with just enough personnel to keep the plant running, so facilities no longer have the extra time, personnel and resources required to analyze the 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, 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 both operating costs and 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 in installed instruments but currently inaccessible – because you didn't know it was there or couldn't afford the equipment upgrades to read it.

HART Protocol

With over 40 million installed HART devices worldwide, HART continues to get updated revisions that continually enhance data exchange capacity, speed, number of devices on a network, support over Ethernet, and wireless capability. It enables 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 endeavours.

In many cases, HART instruments were installed simply because they could be configured and diagnosed easily with a HART handheld communicator (HHC). However, 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. 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).

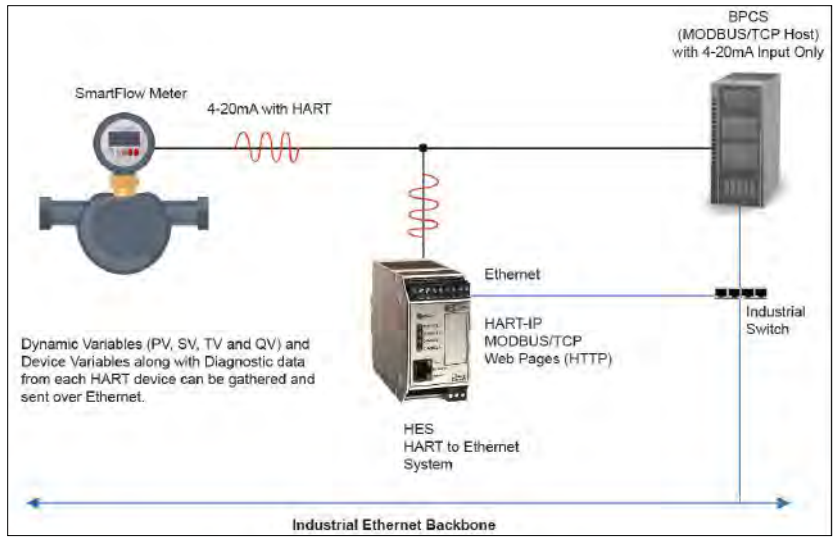


Figure 2. A HART interface device like the HES HART to Ethernet Gateway connects to the 4-20mA process signal and extracts HART process and diagnostic variables and makes them accessible via Ethernet.

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 to 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 which 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, there are standalone HART gateways, which often provide the most economical pathway to extracting HART data from field devices and 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 multi-dropped for maximum data concentration (See Figure 3).

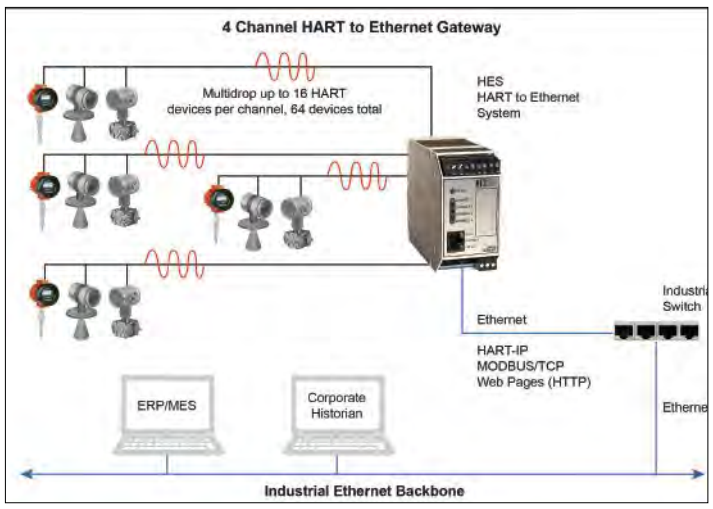


Figure 3. HART to Ethernet gateways offer a quick and economical way of sharing critical HART data with higher level systems.

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.

Employing this HART data for process monitoring, control, predictive maintenance, and process optimization requires that open and vendor neutral industrial protocols be supported. This 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 4). HART-IP devices typically allow for any HART field device data to be mapped to a number of Device Variables locations for reading by a HART-IP host.

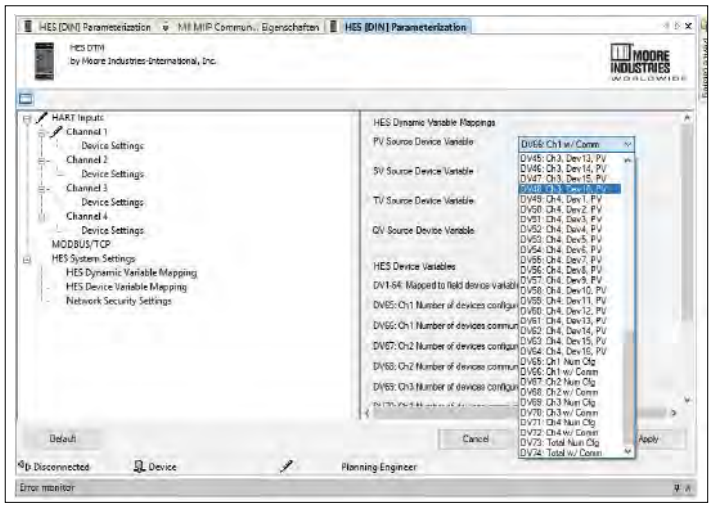


Figure 4. HART gateways supporting HART-IP typically allow freeform mapping of HART field device data.

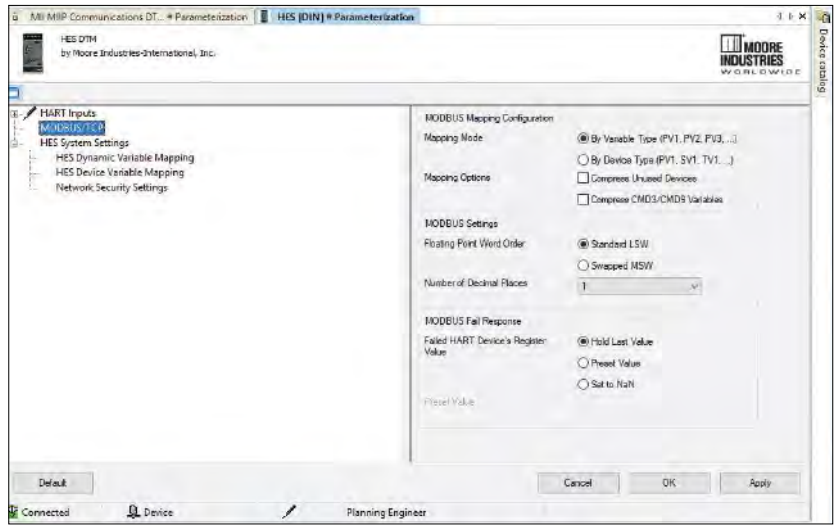


Figure 5. HART to Ethernet gateways should support open industrial Ethernet protocols like MODBUS/TCP.

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 5).

Additionally, Ethernet devices can offer web pages to view the collected HART process and diagnostic data on 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 with easy-to-understand headers and address locations (for other supported protocols) so that additional hosts can be configured more easily (See Figure 6).

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.								

Channel 3								
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 3, Device 1 Addr: 0, CMD3 Tag: HTZ001	32.568 DEG C (65)	362.125 DEG C (193)	369.254 DEG C (321)	12.364 DEG C (449)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 3, Device 2 Addr: 1, CMD3 Tag: HTZ002	92.654 DEG C (67)	123.654 DEG C (195)	368.213 DEG C (323)	326.214 DEG C (451)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 3, Devices 3 to 16 are not polled.								

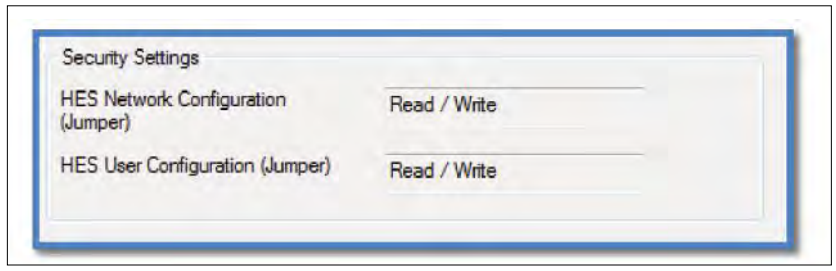
Channel 4								
Device	**1st DV/PV Units (MBReg)**	**2nd DV/SV Units (MBReg)**	**3rd DV/TV Units (MBReg)**	**4th DV/QV Units (MBReg)**	**5th DV Units (MBReg)**	**6th DV Units (MBReg)**	**7th DV Units (MBReg)**	**8th DV Units (MBReg)**
Channel 4, Device 1 Addr: 0, CMD3 Tag: THZ2001	56.324 DEG C (97)	989.236 DEG C (225)	658.359 DEG C (353)	361.326 DEG C (481)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 4, Device 2 Addr: 1, CMD3 Tag: THZ2002	812.536 DEG C (99)	329.846 DEG C (227)	723.362 DEG C (355)	1235.324 DEG C (483)	Not Polled	Not Polled	Not Polled	Not Polled
Channel 4, Devices 3 to 16 are not polled.								

Figure 6. Web servers should display extracted HART data on web pages in easy-to-read tables with optional addressing for other protocols (MODBUS shown here).

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 also be restricted to authorized personnel only and process data should be read only – unless the device is required to perform control. It's important that the entire product lifecycle, including design, build and test, adhere to tight process and quality assurance requirements. Additionally, post-installation considerations should be taken to assist onsite protection of data and property. At a minimum, a two-layer protection scheme should be put in place for the device that includes software and physical hardware restricted access (See figure 7).



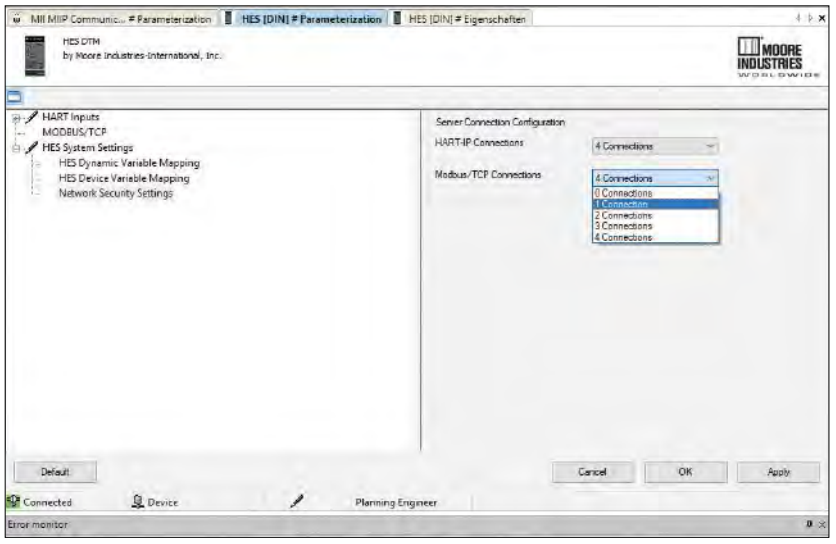


Figure 7. The HES HART to Ethernet gateway restricts unauthorized access with a hardware solderless jumpers and software communication socket restrictions.

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, become familiar with and get IT support and permission.

Most IIoT capable devices are not simple field instruments and therefore small handheld configurators are not convenient for setup 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).

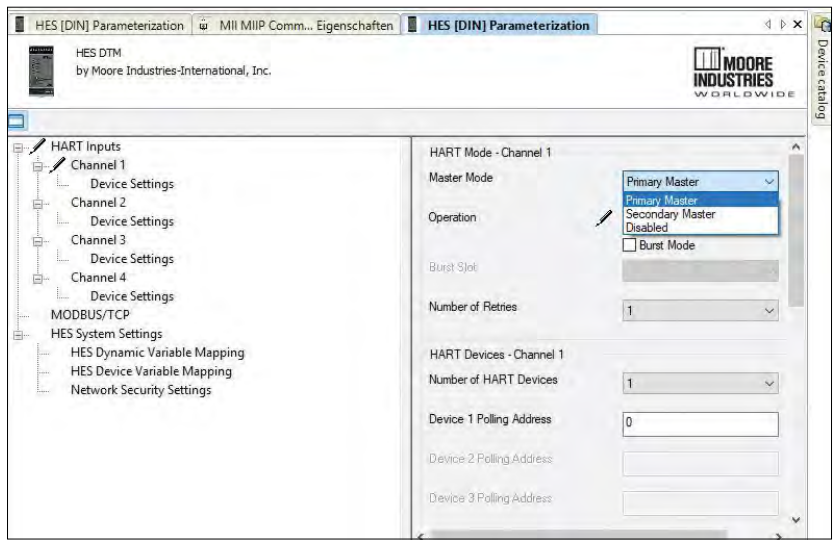


Figure 8. Look for devices that support open industry standards like FDT/DTM technology for programming, so free software like PACTware can be used.

Taking critical plant floor data from smart HART field devices and sharing it with higher level control and information systems, 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.

About the author: T.S. Todd is Director of Engineering at Moore Industries. She has a BSEE from Brunel University and more than 25 years of systems engineering experience in industrial, communications and aerospace applications.

Moore Industries
www.miinet.com