March, 2017

Safety and Security with respect to HART in combination with SIS systems

We live in a changing and fast-moving world. Information is crucial with respect to IoT and Industry 4.0. The amount of data available to us is unprecedented but how to turn that data into usable and secure information often eludes us. How do we access this data, ensure that it is reliable, and turn it into usable information?

HART (Highway Addressable Remote Transducer) is a well-known and widely used protocol in the automation world. It is used to communicate bidirectionally between intelligent field instruments and host systems over 4-20 ma instrument wiring in order to gain additional device information.

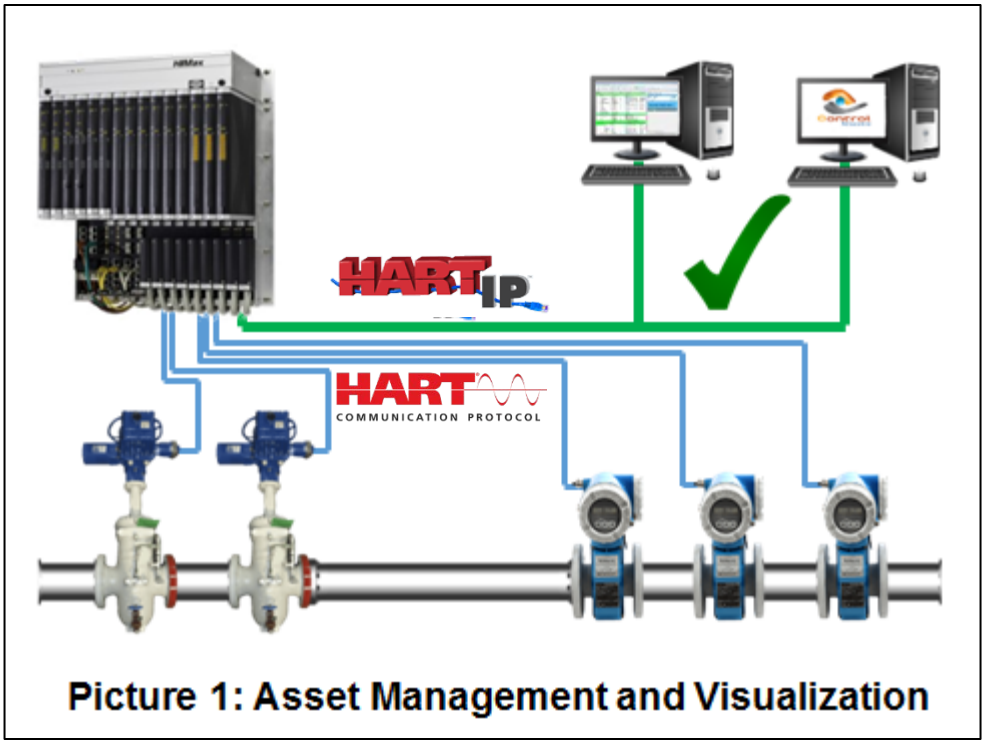
The HART protocol can transmit a lot of information that would be available as an additional diagnostic layer making safety instrumented systems more reliable and secure if we could find a way to access it. At the same time, the use of HART enabled devices creates risks that are often unrealized or under-mitigated. The ability to modify the configuration of a HART enabled transmitter without the knowledge of the safety system is one very obvious example. A user might decide to use devices that are no HART enabled to eliminate this risk but the situation is that most instruments are HART enabled so this elimination could be costly if it would be possible at all.

This paper will discuss the risks involved in using HART enabled instruments in a Safety Instrument Function (SIF), provide a methodology for minimizing that risk, and demonstrate ways that the HART protocol can be used to enhance the reliability of the SIF and the safety of the process.

HART has continued to evolve over its lifetime from a convenient way to calibrate instruments to a more complete diagnostic information highway. Recent enhancements such as HART-IP in the latest HART specifications (Version 7) make it more fit for the future.

HART-IP offers an additional connection option that allows host-level systems and asset management applications to access and integrate measurement and device diagnostic information from HART-enabled field devices using the existing plant networking infrastructure.

As shown in the graphic below, HART-IP can deliver information to higher-level applications (SCADA, CMMS, DCS, ERP and others) from the HART field devices via ethernet.



Picture 1: Asset Management and Visualization

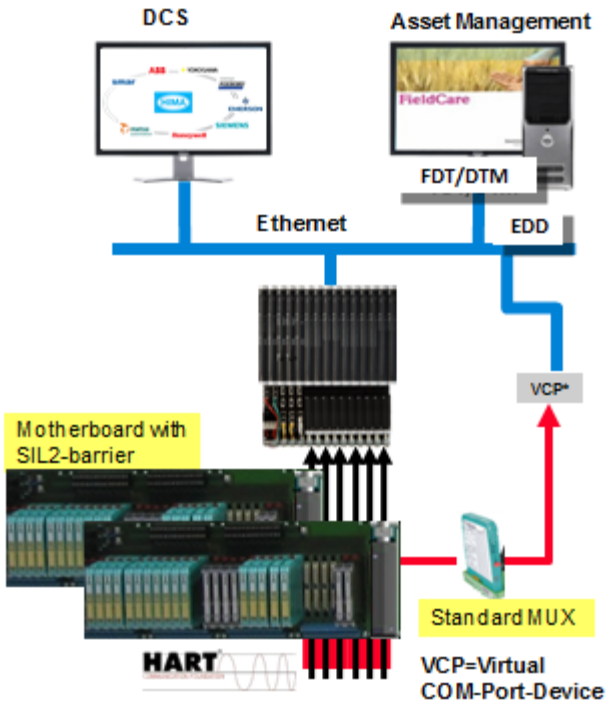
When HART devices are used in safety instrumented functions (SIFs), the HART information is often totally overlooked, and the primary usage of the HART capability becomes to allow for calibration via a handheld calibrator. It should be noted even this innocent use of the HART protocol creates a risk. Any technician can re-configure the HART device which could render the SIF totally ineffective.

If the data is to be collected at all, there are two conventional ways to extract the HART information from the field devices.

1. The HART signal is extracted from the 4-20 ma line via barriers/decoupling boards and sent through a MULTIPLEXER device BYPASSING the Programmable Electronic System (PES) directly to the Asset Management System (AMS). In this case, the PES plays no role in the HART communication, and all necessary actions concerning HART rely on external devices. All known MUX solutions use RS-485 communication to the HART host.

   While this methodology gets the information to the AMS system, it should be noted that it can also create issues. For instance, the AMS could write a new configuration to the instrument, modifying its calibration and making the PES system totally ineffective.

   So, while the use of a multiplexer gets the HART information to the AMS and makes it useful, it also creates or amplifies issues surrounding the use of HART in a SIF.

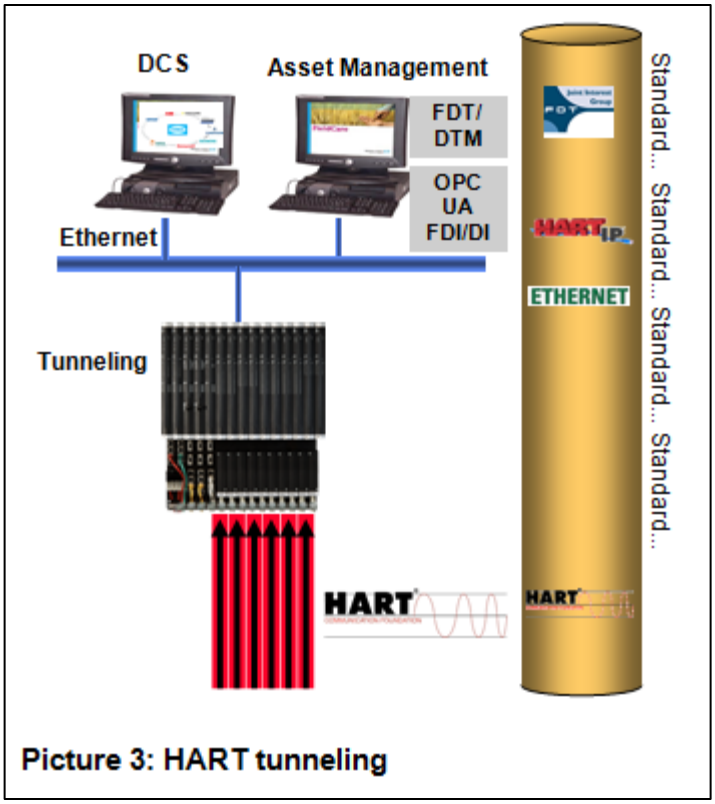


Picture 2: HART signal extraction via Multiplexer

2. A more recent methodology for extracting HART data is the “HART pass-through” or “tunneling” methodology. In this case, the HART information is read into the PES via I/O modules that have HART functionality. Communications from the PES to the AMS could use either HART-IP or RS-485 to transmit the information. Since all of the HART information is transmitted from one central location, this methodology can be implemented more easily.

   However, upon examination, HART tunnelling does not solve any of the problems previously cited. The instrument configuration can still be changed by the AMS or with a handheld calibrator without the knowledge of the PES. These changes could still make the PES totally ineffective.

It should be noted that most end users have policies and procedures that would prevent modification of field device parameters for devices involved in SIFs. But it should also be noted that these procedures rely completely on the personnel involved always understanding and following these procedures.



Picture 3: HART tunneling

To reiterate, no matter which communication method is used, the HART information does not in any way interact with the SIF. It either bypasses the PES altogether, or it is tunneled through the PES directly to the AMS.

Before we proceed any further, it should be made clear that HART is not a safe protocol. This is why the PES is bypassed in conventional applications. Additional measures should be considered if the data is to be used in safety-related systems. These measures have already been discussed in a TÜV whitepaper* that was published in 2008 and is cited below.
On the other hand, it seems obvious that the usage of the HART data in the PES could provide benefits. Usage of HART in combination with a PES can leverage your plant performance while still maintaining safety AND security, but data flow to/from a safety system always has to be supervised and controlled in a safe and secure manner.

If we for a minute assume that there is significant value that could be derived from the use of HART data to make the SIF more reliable, but we know that HART creates some vulnerability, is there a way that we can have our cake and eat it too, so to speak?

Before moving further, let's look at basic care needed when using HART in a SIF.

1. The HART signal is a superimposed frequency signal that rides on the 4-20 ma signal. It has an amplitude of +/- 0.5 ma. The potential inaccuracy created by the HART signal must be considered in the SIF configuration. The PES manufacturer should state in its safety manual the influence of the HART signal. See the sample extract below.

- HART communication influences the analog metrological accuracy by approx. 1 %. There are no additional repercussions for the analog modules.

2. Another concern is the possible impact of the decoupling of the HART signal and the 4-20 ma signal. Again, the safety certificate/manual should indicate the non-interference of the HART signal with the 4-20 ma signal. The user should ensure that the non-interference is certified to the SIL rating required of the SIF and that this certification is done by a reliable and trustworthy third party. If the non-interference cannot be assured, it may be necessary to decrease the SIL capability and/or shorten the proof test interval, possibly to an unacceptable length.
3. Finally, the HART field devices must be suitable for the required SIL rating. And the documentation should state the non-interference of the HART and 4-20 ma signal on the device level. The user must be assured that a failure in the NON-SAFE hardware/software part, which generates/handles the HART signal, must not have any impact on the SAFE 4-20 ma signal.

Issues 1 through 3 above are easily mitigated by dealing with responsible vendors who achieve and maintain the required certifications. This leaves only the most daunting issue: how to control configuration changes to the device during service, either intentional changes or unintentional changes.

Let's start with the simplest case. In many safety applications, the HART data is not archived in any manner. HART is simply used to configure the instruments, using a handheld HART configurator. While this activity is usually covered by established procedures and reconfiguration requires a password, is that sufficient? Usually, passwords are fairly weak (4-6 digits), and they must be known by a number of people as they will be needed if an instrument fails or needs to be replaced. Consider the number of devices at a typical site and the fact that individual passwords are impractical and it seems obvious that too many people know the password for us to accept that as a preventive measure.

Often, reconfiguration is protected by a DIP switch, but the switch is typically on the non-safe HART side of the device. Can we really take credit for unintended device changes if a non-safe DIP switch is the only protection?

Even if an asset management system with better security measures is employed, it doesn't prevent changes from a handheld device and, if information is to be written from the AMS to the device, the DIP switch protection must be overridden.

Even with all of these concerns about the use of HART in safety applications, it is a fact of life that most of the devices used in safety applications are HART enabled. As an industry, we're left with the options of continuing to put our heads in the sand or finding a way to alleviate the concerns.

Now consider the many arguments in favor of using HART information as an add-on to safety features and the possible creative uses of HART data in the safety application for improving safety, availability and reliability.

The TÜV paper cited earlier states that, in general, online changes, online calibration and online maintenance/repair in safety-related applications based on the HART protocol should be avoided and must be evaluated case by case. But there are system solutions available in the market to address the possible issues.

One possibility would be to allow HART communication from the AMS through the safety system to the field device only in specific situations and plant states (e.g., during a shutdown, turnover

or field device failure). The HIMA HIMax HART tunneling solution allows the user to enable and disable write protection by means of variables in SIL quality and covered by the certificate of the system. This capability would avoid unintended configuration changes from the AMS.

The TÜV paper also states that HART information can be used for device diagnostics and maintenance purposes to identify potential failures of field elements that might prevent the safety function from acting if demanded. In this case, the HART information would act as an additional diagnostic layer of protection.

The HIMA HIMax solution allows the HART information to be read into the PES and used to detect such things as:

- The HART diagnostic that indicates that a device has been reconfigured. On learning this, the HIMax could be configured to take that element out of the vote, provide notification, shut the system down or take any other user defined action.
- The flat line diagnostic that indicates that the device is inoperable. Again, this information could be used to take corrective action.
- The PV via HART to confirm the value being received by the 4-20 ma signal. While, as pointed out earlier, HART is not a safety protocol, it can be used to confirm information. Knowing that the measured PV and the HART PV do not agree would allow the HIMax to notify the operator to investigate.

Knowing any of these things would allow the PES to alter the logic, to generate an alarm, to take the system to a safe state or to do any combination of these things, making the PES smarter and the SIF safer.

Thus this paper makes the case that HART can and should be used in conjunction with PES's in safety applications. It also makes the case that, as HART devices are already being used without the assurance of proper supervision, there are risks to the proper operation of current safety applications that are not well managed.

- HART signals should always be collected in safety applications.
- They should be "tunneled" through PESs that have the ability to prevent the AMS from writing to the devices except in certain instances.
- Diagnostic data should be collected in the PES to at least assure that the devices calibration has not been modified and that the device is operable

In short, HART should be used in safety applications in a manner that makes the safety function more reliable.

As stated earlier, the ability to read HART data into a PES opens the user up to myriad applications limited only by his/her own creativity. Some possible applications are described below, but users should employ their own imagination and knowledge of the application to put the data to best use in a given application.

1. Use device diagnostic information (potential failures, upcoming failures) inside the SIF logic. Of course, this information is not safety related, but it can be used inside the SIF logic as an independent, additional layer of protection. A device failure can be used to react in a different way than the case of a real limit value violation, e.g. take this measurement out of a voting logic. Or, some devices (e.g., gas sensors) can notify via

HART that they will fail in the near future, giving the plant personnel the chance to react in advance.

2. Use the HART signals for plausibility checks. Comparing the 4-20 ma signal versus the HART PV provides further diagnostic capability.
3. Check for configuration changes inside the PES. One major impact mentioned several times previously is an unintended configuration change. But as standard information, any HART-capable device must deliver via HART the “configuration changed flag.” This flag is set in the device if any single setting in the device is changed. By reading it into the PES logic, an automatic reaction can be taken inside the PES.
4. Create special applications to manage assets or provide statistical evaluations. Sometimes dedicated AMS systems might be “oversized.” Data can be analyzed inside the PES or transmitted to another system or HMI for analysis.
5. Perform device configuration cross-checks. Depending on the HART capabilities of the safety system, it could be possible to check the device configuration, e.g., read the measurement range via HART into the PES program and compare it to the configuration of set points inside the safety system.
6. Store the configuration of a device inside the PES ensuring that if the device is replaced, the exact same configuration can be downloaded to it replacement.
7. Change the configuration of a device depending on the process step or situation to get more exact information.
8. A safety system with full HART capability, which is able to process not only any HART command but which also includes device-specific commands, can do even more. From managing partial stroke testing to monitoring the “heartbeat” that some instruments are capable of providing, the possibilities are endless.

World’s first HART solution with TÜV-certified write protection and HART filtering in SIL 3 quality

HIMA’s new HART solution allows the safety system to access the HART parameters. This enables operators to use device diagnostic information (e.g., about potential failures, upcoming failures) inside the safety instrumented function (SIF) logic. Although this information is not safety related, it can be used inside the SIF logic as an independent, additional layer of protection. Gas sensors, for example, can notify via HART that they will fail in the near future, giving plant personnel the chance to react in advance (predictive maintenance).

The HART solution contributes to increased plant safety by allowing the system to monitor configuration changes – even if made via handheld devices. This information can be used to modify logic, to bypass disabled devices, or to initiate a shutdown. Furthermore, proof tests such as partial stroke tests for valves can be initiated and managed from the safety system.

With existing HART solutions, it is possible for personnel (or external hackers) to reconfigure the field devices via the Asset Management System. This poses a major cybersecurity and safety risk.

If, for example, a limit value of a SIF (safety integrated function) is set to 75% of a measuring range of 10 bar, and someone changes only that range within the sensor to 100 bar, the ESD is triggered only when the level of 75 bar is reached – meaning the SIF will fail to do its job, causing major safety and production problems.

HIMA's HART solution closes this security and safety gap in today's process industry. By channeling communication through a safety PLC featuring enhanced security—instead of through a separate HART multiplexer or by standard tunneling as is currently the norm—the communication benefits from the additional firewall. The firewall allows data reading but prevents data writing/configuration and the direct access to field devices from the Asset Management System.

Conclusion

This paper posits that the use of HART in SIFs is not really optional, as most of the instruments in use have HART capability.

It is incumbent on the user to find a verifiable method to ensure the integrity of the 4-20 ma instrument signal in the presence of the HART telegram.

It is also the responsibility of the user to ensure that the configuration of the device is not modified without the PES being informed and reconfigured to accommodate the modification or to take the proper action.

It is possible to manage the concerns about the use of HART to prevent and/or be aware of unintended calibration changes, and to use HART data and diagnostics to make the SIF more secure by using HIMax Safety Systems.

**Referenced document - TÜV paper - "Position paper about the use of HART Communication in safety related application within Safety Instrumented Systems" - Dated 2008, Author Mr. Busa*

About HIMA

The HIMA Group is the world's leading independent specialist in solutions for safety-critical applications. With more than 35,000 installed systems and TÜV-certified hardware and software, HIMA qualifies as the leading technology company in this sector. For over 45 years, the world's largest oil, gas, chemical, pharmaceutical and energy-producing companies have relied on HIMA products, services and consulting to provide uninterrupted plant operations and protection for people and the environment. HIMA solutions are also leading the way to increased safety and profitability in the rail industry, logistics and machine operations. An independent family-owned company, HIMA operates from over 50 locations worldwide, has a workforce of approx. 800 employees. For more information, please go to www.hima.com

Authors

Bernd Schaefer
Product Manager OPC, SCADA, HMI
HIMA Paul Hildebrandt GmbH
Bruehl, Germany

Buddy Creef
Sales Director
HIMA Americas, Inc
USA, Houston, TX

Contact HIMA Americas

HIMA Americas, Inc.
5353 W Sam Houston Parkway N., Suite 130
Houston, Texas 77041, USA
Phone +1 713 482 2070
info@hima-americas.com
www.hima-americas.com