TECHNICAL ARTICLE
HART COMMUNICATION PROTOCOL

HIMA
SMART SAFETY.

Increased data security and manipulation protection with HART-capable field devices

Bernd Schäfer, Product Manager OPC/SCADA/HMI
Alexandre Terentiev, DCS Expert – TÜV Functional Safety Engineer #3956/11, SIS at HIMA

The digitization of field devices offers huge potential for plant operators to reduce operating costs and increase productivity. Highway Addressable Remote Transducer (HART) based field devices, however, carry significant risks of tampering and their configuration is comparatively error prone. By channeling communication via a SIL 3 safety controller, plant operators can now use the data from such field devices for diagnostic and process optimization purposes without safety or security risks.

With over 40 million field devices installed and support from leading instrument suppliers, the HART communication protocol is today the most widely used digital communication technology in the process industry. Although the HART signal has so far been used predominantly for parameterization, with the appropriate tools it can enable continuous device monitoring and diagnostics as well as multivariable process information.

Up to now, it has been difficult or even impossible to obtain truly useful data in safety-related applications. The problem: Although many field devices are now equipped with the HART protocol, in most cases these are only used during commissioning. In addition, conventional HART communication is susceptible to manipulation and misconfiguration – especially during operation.

HART communication – a security risk?

Conventional HART communication in safety-related field devices – usually done via a separate HART multiplexer or standard tunneling – involves significant safety risks. This is due to the fact that the safety system is more or less completely bypassed and doesn't notice the HART communication. As a result, potential cybersecurity risks arise, as employees may be able to change instrument parameters of field devices unintentionally or hackers may do so deliberately, which can endanger the safety and availability of a plant.

For example, if a Safety Instrumented Function (SIF) limit value within the safety controller is set to 75% of a measuring range of 0 – 10 bar (equivalent to 4 – 20 mA) and someone changes this range to 0 – 100 bar only within the sensor, the corresponding reaction is only triggered when a measured value of 75 bar is reached – which means that the SIF does not perform its function and can cause significant safety and production problems.

New HART Solution offers comprehensive diagnostic capabilities

HIMA has developed a HART solution that, for the first time, enables the implementation of comprehensive diagnostic options at the field level in HIMax safety systems. The solution enables important information to be transferred from the field devices to both the asset management system and the user program via the HART protocol.

The innovative solution consists of the HIMax module X-HART 32 01 (image 1) and the HIMax-HART package. The 32-channel HART module can be installed alongside any AI/AO without additional wiring requirements. It enables centralized access to the HART information of the field devices connected to the HIMax system. The module can be inserted in any slot of a HIMax base plate, with the exception of those for system bus modules. It can be combined with analog input or output modules in a mono or a redundant version through the use of connector boards (figure 1).

HIMax HART module X-HART 32 01.

Figure 1

The HIMax HART software package allows HART data to be utilized in the user program, supplies a predefined function library, and can be extended with further libraries. It includes import files for predefined HART variables via a preprogrammed communication driver plus a predefined block library for selected standard HART commands (15 are implemented at present). Specific commands of each device manufacturer can be implemented quickly. Tasks such as individual evaluations and reports, which were previously very time-consuming, are considerably easier.

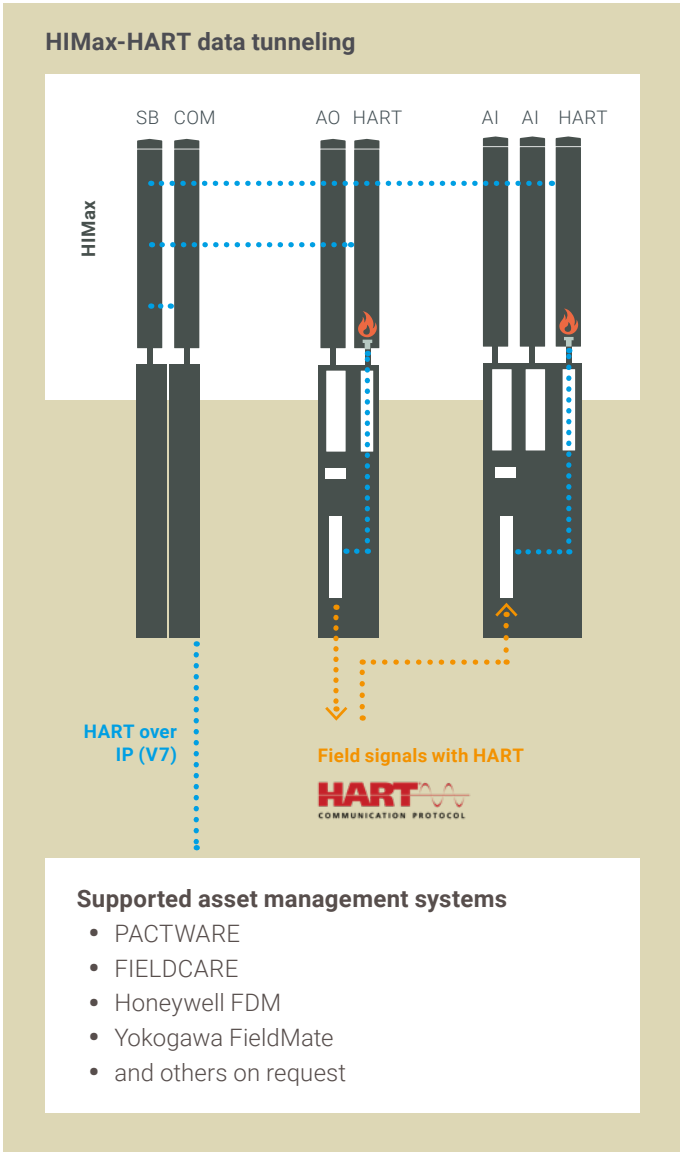

Figure 2: HIMax HART data tunneling

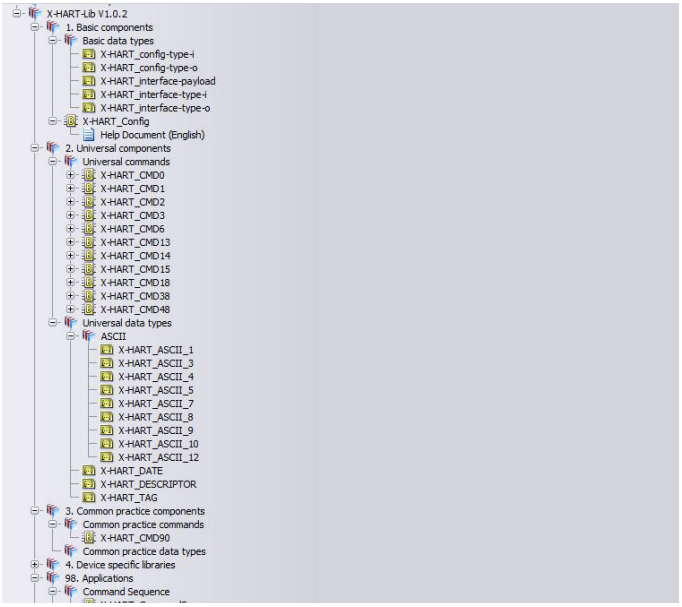

Figure 3: HIMax HART software package.

Secure communication channel

HART data from field devices is channeled via HIMax for increased safety and security (figure 2). In this process the data is transmitted from the X-HART modules via the internal system bus to the assigned X-COM module. From there, they find their way into the asset management system or the HART-OPC server via HART over IP protocol.

Channeling the HART communication via the HIMax safety controller – this includes “listening in” to HART communication and the option of restricting or preventing unwanted communication in SIL quality – ensures secure and protected asset management. This is more or less comparable to the “Deep Packet Inspection” function of an Ethernet firewall. Channeling ensures that the device values can only be changed via the safety PLC (with the exception of handheld devices). This is the only solution on the market with complete control of the HART communication traffic with SIL 3 quality in accordance with IEC 61508, IEC 61511, and IEC 62061.

The additional possibility of monitoring changes to configuration, e.g., on site with the device or with handhelds, allows manipulations to be prevented or at least detected so that an appropriate action can be taken. This extra degree of cybersecurity eliminates risks when using HART devices in safety applications, which were previously common. It is also possible to initiate and administer proof tests such as partial stroke tests for valves or complete proof test routines for sensors from the safety system.

Increased protection against manipulation

The security features of the safety controller make it possible to achieve a security concept in accordance with IEC 62443 for HART device access. These features include separate communication pathways in the system for secure and non-secure data as well as clearly defined communication ports. They also contain an integral HART filter in SIL 3 quality, which “listens” to the data traffic and can be controlled to only allow read access to the field devices, or it can block all write commands. This combination of complete flexibility and security features makes the automatic repeat test according to NAMUR NE106 possible via the safety controller, even for SIL locked devices in protective devices in an installed state.

Combined with HART devices, the HIMA HART solution increases security. Unauthorized changes to the device are detected or prevented immediately by write protection. This reduces the risk of cyberattacks causing damage. The additional possibilities for blocking and filtering in SIL 3 quality and the possibility of monitoring with reference to configuration changes for SIF field devices ensure that the plant is protected against manipulation. This applies to both unintentional configuration changes such as operating errors and to intentional attacks by hackers. The HART solution from HIMA therefore closes an important safety loophole in the process industry and enables the acquisition of diagnostic data from field devices in safety circuits. Plant operators can make this diagnostic data acquired with field devices easily and securely usable for the asset management system.

TECHNICAL ARTICLE
HART COMMUNICATION PROTOCOL

For further information please contact:

HIMA Paul Hildebrandt GmbH
E-mail: applications@hima.com

Or visit us online:
www.hima.com/en/industries-solutions/overview-of-all-hima-solutions/hart

HIMA SMART SAFETY.

www.hima.com