WHA-GW WirelessHART Gateway

Software 2.0 Release Notes

NAMUR version: 02.00.01

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Document Scope

This document refers to the SW version **2.0** (HART Software Revision Level 2) of the WHA-GW WirelessHART Gateway device, which provides an EtherNET-IP communication interface.

The document describes the new capabilities and the functional improvements associated with the new SW version.

Moreover, the document lists all the HART commands supported by the Gateway at the wired interface level identifying the commands that were either added or modified with this SW version.

1.2 Summary of Changes

The most relevant changes associated with this SW release are shortly described in the following.

- **Whitelisted Security Mode**

  The Gateway now fully supports the “Whitelisted” wireless security mode; when this mode is enabled, only the whitelisted wireless devices will be allowed to join the network, increasing the level of security to an optimal level, especially when coupled with the join-key change procedure described later-on.

- **Wireless-level Join Key Change**

  An optimised and reliable procedure is now available to change the join-key of all wireless- connected devices. The procedure will proceed in the background, without interfering with the normal devices operation. It will be possible for the user to monitor the progress – and the successful completion – of the change procedure and to recover from any possible failure (e.g. a device temporarily loosing wireless communication during the change).

- **Advanced Cache Management**

  The number of commands cached within the Gateway was substantially increased. This is useful both to support the the new functions associated with this SW release and to reduce the Gateway response time to Host application requests.

  In addition to caching all published burst responses, the Gateway now caches also the information associated with all of the following read commands:

  – 0, 11, 21, 13, 15, 20, 38, 50, 74, 84, 101, 105, 64394.

  The cached information for these commands is always kept consistent and up-to-date, both by automatically monitoring – and resetting – the Configuration Changed flag at the device level and by “intercepting” relevant any host-received “write configuration” command.

- **Special Operating Modes**

  It is now possible to selectively disable some “automatic” procedures executed by the Gateway in the normal operating mode. This can be very useful both in commissioning phase and to properly support some special, application cases.

  In addition, the Gateway now support a special “Wireless Broadcast” mode which can be useful for a faster, parallel acquisition of critical devices information in some special cases.

- **Performance Improvements**

  The performances of the Gateway were improved in many areas, and more specifically:

  – The Web IF response-time was reduced.

  – A 100ms publishing period is now supported at the wireless level

- **Protocol Improvements**

  The HART-IP protocol was improved in a few specific areas, and made more flexible.

- **Stale Data Detection**

  The Gateway can now verify that published values are really received from each wireless device at the expected rate. This enable a timely detection of any of wireless communication problems, with the generation of suitable “Warning” and “Error” indications. This capability is fixed and it is not yet available on the EtherNET-IP communication interface.

  All kinds of BURST trigger modes are supported to perform the stale detection.

- **Security Update**

  The Web Interface is no longer vulnerable to the Path Traversal attack.

➢ **Improved Identification procedure for a device**

The cache of commands is checked before send the particular identification command.

The CCF reset procedure as well as the SDLC procedure have improved to speed up operations and to save the usage of wireless bandwidth.

➢ **Pass-Through Mode**

The HART Pass-Through Mode is natively supported. It's possible to send a command directly addressing the listed sub-device.

2. NEW FEATURES

2.1 Stale Data detection

The Gateway can now measure the "age" of each cached CMD 48 or Dynamic Variable. If the measured age exceeds a fixed threshold, a "Warning" or "Error" indication is be generated. The "age" is available information either as a % of the burst period or as direct time value.

To make "stale-data" detection possible, the Gateway will time-stamp each received published message.

Stale-data detection is supported for any Dynamic Variable received within CMD 3, CMD 9 or CMD 33.

The thresholds are fixed as follows:

- Warning: 150% of quickest Burst period
- Error: 300% of quickest Burst period

The Gateway can keep updated the Burst settings automatically.

All the available kinds of BURST trigger modes are supported to perform the stale detection.

2.2 Network Security support

➢ **Whitelist support**

The Gateway now supports the "Whitelist" wireless security mode; when this mode is enabled, only the whitelisted wireless devices will be allowed to join the network. One new command (185) was defined to support the "Whitelisted" security mode – which is also based on the usage of four standard wireless commands (814, 816, 821, 822).

➢ **Wireless-level Join Key change**

It is now possible to modify the join key of all wireless-connected devices without the need of reforming the network – and without the risk of permanently "loosing" a device in case of a key-update failure.

During the key-change, the Gateway will keep track of any wireless device for which the key update failed; it will then be possible to recover the situation by using a new "Temporary Join Key" mode (which activation status is also reported within CMD 48).

Four new commands (149, 164, 192, 187) were defined to support the "Join Key change" procedure – which is also based on the usage of a standard wireless command (848).

Command 192 can be used to monitor the progress of the join key change activity, which also appears as a new flag within existing status commands (145, 148).

Warnings:

- All the devices within the Whitelist share the same join key and are identified via their HART Unique Id.
- To avoid any undesirable side-effects, the GW will not allow a Host application to directly use command 768 so change the Join Key of a single wireless device.

2.3 Substitution Values management

In case of wireless communication problems, the device variable values can now be substituted with NaN2 value. The "substitution" takes place either if the device is reported as "disconnected" from the wireless network or when a "stale-data" error is detected for a variable.

2.4 Burst Configuration Caching

The full burst configuration of each wireless device is now cached within the Gateway. This is useful both to support the "stale-data" detection and to reduce the Gateway response time to Host application requests.

During the identification phase, following commands will be used to fill the burst-configuration cache:

- CMD 105 (Read Burst Mode Configuration) → Sent to all wireless devices.
- CMD 101 (Read Sub-Device to Burst Message) → Sent only to Adapter and Discrete wireless devices.

To keep the cache up-to-date the Gateway will also track the responses to all the "burst-configuration" write commands (CMD 103, 104, 108 109).

Warning:

If Burst Configuration caching is disabled by using CMD129 (Set Special Operating Mode) all "stale-data" Gateway functions will also be disabled.

2.5 Additional Cached Commands

The number of commands cached within the Gateway was substantially increased. This is useful both to support the the new functions associated with this SW release and to reduce the Gateway response time to Host application requests.

The following table show a list of all Gateway-cached commands, showing in bold the new ones.

CMD	Description	Primary caching reason
0	Read Unique Identifier	Faster Host-application access
11	Read Unique Identifier Associated With Tag	Faster Host-application access
21	Read Unique Identifier Associated With Long Tag	Faster Host-application access
13	Read Tag, Descriptor, Date	Faster Host-application access
15	**Read Device Information**	The Web IF needs to display a non-standard unit code (e.g. as in the EthernetIP case).
20	Read Long Tag	Faster Host-application reading
38	Reset Configuration Changed Flag	CCF reset & Cache management
50	**Read Dynamic Variable Assignments**	Stale Data management
74	Read I/O System Capabilities	Instrument List management
84	Read sub-device identity summary using list index	Instrument List management
101	**Read Sub-Device to Burst Message Map**	Stale Data management
105	**Read Burst Mode Configuration**	Stale Data management
64394	**Read Burst Discrete Variables**	Discrete I/O support

Note:

In addition to these commands, the Gateway also caches all published burst responses.

2.6 Special Operating Modes management

In the normal operating mode, the Gateway automatically executes, as a background activity, a series of "automatic" procedures.

The Gateway now allows to disable one or more of these procedures by using command 129. This can be useful both in the debugging/commissioning phase and to support special application cases.

2.7 Improved Identification procedure

A device “identification procedure” is required to fill all the relevant Gateway cache entries – and to keep them updated and consistent in case of a configuration change. The Gateway executes the “identification” procedure each time a wireless device joins the network and whenever a “CC flag set” condition is detected.

The identification procedure was made faster and more reliable; for instance, it is now possible to send HART commands also to a (joined) wireless device while it has an ongoing “identification” phase.

In order to make the identification procedure more efficient – and to avoid to interfere with the normal configuration messages – the Gateway now default to the “***best-effort***” wireless mode to transfer the identification-phase messages. However, the Gateway is smart enough to fall-back to the “***reliable***” identification mode if the “best-effort” one is not supported by a specific device – or if there are communication problems with the device.

The information regarding the device capability to support wireless aggregation is now persistently stored to speed up operations and to save the wireless bandwidth for the next power-up and reset requests.

Note:

If a joins with a Long Tag that is already listed for an off-line device, the new device will “substitute” the original one without reporting a Long Tag duplication error. This simplify the replacement of a “faulty” device with a new, identical one.

2.8 Performance-related improvements

In addition to what previously described, the performance of the Gateway improved in various specific areas, as described in the following.

- **Real Time Clock update**

  CMD 89 execution time (in the DR mode) is now faster and fully reliable.

- **Lists rebuild**

  The “Apply Instrument List” and “Rebuild List” procedures are now executed without interrupting the normal Gateway operation; moreover, no device re-identification is now required after the procedures end.

- **Network Manager Communication**

  In case of temporary communication problems with the internal Network Manager unit, the Gateway can now still answer to HART requests and execute a limited number of operations.

- **Web IF performance**

  A series of commands (159, 184, 188, 190, 774 798, 817, 822, 843) return an immediate answer (DR mode support removed); this reduced the Web IF response time.

- **Wireless communication**

  The “P1” wireless bandwidth profile was improved and it is now a bit “faster”. Moreover, some parameters were modified so that a burst period down to 100 ms is now supported for low-latency applications.

2.9 Pass-Through Mode

The HART Pass-Through Mode is now natively supported. For a host it is possible to send a command by directly addressing the listed sub-device, i.e. without the need to use the CMD77.

3. ADDITIONAL IMPROVEMENTS

3.1 Web IF User Levels

The Web IF now supports two distinct user-access levels.

"Operator" User Level:

With this access level, no access password is required and no "Inactivity Timeout" applies. However, the User is not allowed to modify any configuration parameter.

"Administrator" User Level

With this access level, a password is required and an "Inactivity Timeout" applies. However, the User has full access to all available Web IF capabilities

3.2 Software Upgrade Procedure

The Web IF software upgrade procedure was improved and made more reliable – e.g. the SW upgrade is now not interrupted also if a web page is changed or closed.

3.3 HART-IP protocol

- For higher flexibility, the number of supported UDP sessions was increased from 2 to 4.
- The TCP keep alive mechanism is now enabled.

The "Inactivity Close Time" support is now available also at the TCP-IP level. When the requested value is 0, the inactivity close time adopted by the Gateway is changed to 60 seconds. The inactivity close time set to 0 is accepted for TCP only.

3.4 Command 75 & 77

- Command 75 is now fully specified and supported – and can be used for wired-device polling.
- Command 77 can now support a wireless "broadcast" mode (intended for special application cases).

3.5 Identification procedure improved

The identification procedure has been changed by aiming to have a proper coexistence between the operations performed by the Gateway as a master and those performed by a Host, without any further interferences on both sides.

In order to speed up operations and save the wireless bandwidth usage, the command cache is checked before to send the following identification command requests:

- CMD0
- CMD20
- CMD13
- CMD15
- CMD50
- CMD101
- CMD105
- CMD64394

The identification of a wireless device is now always guaranteed by means a forced identification which is started when the procedure has been never executed within a specified timeout.

In order to retrieve all the required data necessary to perform specific operations (such as the stale detection, and variable mapping), the Gateway sends to the all connected wireless devices a well-defined series of commands (as can be read above); this volatile data is stored in a specific device data structure. The gateway can now keep the devices data structure updated when it receives also the related write commands. The cache of related reading commands is kept updated as usual.

The CCF Reset procedure, for wireless devices, has been optimized to save the usage of wireless bandwidth. There are now 2 procedures:

- The Extended way: The first identification level is executed (i.e. CMD0, 20, 13, 15 are requested), and the variable mapping and burst settings are retrieved. The sub-devices list of an adapter is no longer retrieved, since the variation of instrument list doesn't raise the CCF (the modification of the Long Tag or Message of a wired device must trigger an adapter to raise the SDLC flag).

At the end of the first identification level, the CMD38 is sent to reset the CCF.
This procedure is triggered by any BURST, and the ACKs which are not used by the Gateway to keep the devices data structure updated.

- The Fast way: Just the first identification level is executed.
  At the end of the first identification level, the CMD38 is sent to reset the CCF.
  This procedure is triggered by all the ACKs which are used by the Gateway to keep the devices data structure updated (e.g. CMD51, CMD103, and so on).

The SDLC procedure, for wireless adapter devices, has been optimized to save the usage of wireless bandwidth. The first identification level is executed, followed by the retrieving of the new sub-devices list. The already collected variables mapping and Burst settings are kept.
When the Gateway is retrieving the sub-device list of an adapter during the normal identification procedure and the SDLC is found set meanwhile, the automatic SDLC procedure is no longer triggered, to avoid to repeat same operation twice. The sub-device identification is terminated when the "Invalid Selection" code is received as a response of CMD84, or it is interrupted when other error codes are received.
The duplication of Long Tag for wired devices is now resolved also when the CMD84 response is processed during the normal identification procedure.

3.6 Usage of cache for aggregated wireless requests

By means the device specific command 182 “Read Aggregated Wireless Information” is possible to send aggregated commands to a wireless device. It’s now possible to give immediate response by using the cache, but only a full matching is found between all aggregated requests and their correspondent cached responses.

3.7 Other improvements

- The DR mode support was added to a few commands (134, 136, 153, 139) so to comply with the HART-specified response time.
- The Command Line Interface (CLI) was extended to support most new features.
- Improved the procedure used to establish the session with the Network Manager, in order to cope with variable booting time after the device has been powered-up.

4. BUG FIXES

4.1 Firmware upgrade

- The feature to recover a corrupted package of ACD doesn't work. Fixed.
- The feature to recover the passwords and set them to default values doesn't work. Fixed.

4.2 Web Interface

➢ **Security Update**

The CGI of Web Interface was affected by the Path Traversal attack.
When a request to operate on a file is received, the real path of the target file is found by resolving the "../" and "./" possibly present in the path. Then, if the resolved path doesn't match with the working directory, the request is discarded. If the file with the resolved path doesn't exist in the working directory it will be created, as in the case of configuration exporting.
The web service files, can be accessed by specifying only the defined GUID. They cannot be accessed by specifying their path, so an attacker cannot either read or modify them.

➢ **Instrument list representation**

- The channel of I/O System is shown as 1 instead of 251. Fixed.

4.3 EtherNET-IP Process

➢ **Bullet Wired Device Lost Problem**

The EIP process sends commands to wired devices with a number of preambles fixed to 5. Fixed.

Solution: the number or preambles to be sent is retrieved by the command 0 response.

➢ **No HART-IP session-close request sent in case of assertion**

When an assertion is raised, the EIP process is terminated without sending the HART-IP session-close message to the Gateway, and this generates a loop with no end.

It's not possible to fix it in the EIP process, unless to plan a refactoring, so as a solution the Gateway process can now automatically close the established session when a session-init request is received from the allowed EIP masters.

➢ **Changed behavior on busy response code**

The handling of busy conditions leads to generate many assertions, causing a not stable condition to the EtherNET-IP clients. Fixed.

Solution: No action is taken when a busy error code is received for more than the foreseen timeout.

This choice might delay the global identification, but in any case the Gateway guarantees that the busy error code is not returned forever.

➢ **Memory Pool resizing**

When more than 100 devices are connected to the network the EtherNET-IP process crashes. Fixed.

Solution: The number of chunks used by the memory pool, has been increased from 500 to 2500.

This because, since 7 chunks are required for each device, with a maximum number of 500 chunks only

98 devices can be supported. If more chunks are required the process crashes.

The Gateway can support up to 250 wireless devices plus possible wired devices in case of adapters, for instance: 250 adapters with 15 sub-devices each, leads to have up to 4000 theoretical total devices.

With 2500 chunks is possible to support up to 350 devices.

The higher is the number of chunks, the more RAM is consumed; so 2500 is a balanced solution.

4.4 Other bugs

- The persistently stored topology map was not correctly loaded at the boot.
- The communication status of operational motes was not updated after a communication drop with Network Manager

5. SUPPORTED COMMANDS LIST

In order to support the new capabilities associated with this release, some new commands are now supported – and some existing commands were modified.

The following list shows all the commands supported by the Gateway. Commands added with respect to Gateway Revision 2 are marked as (●); commands modified with respect to Gateway Revision 2 are marked as (♦).

5.1 Universal Commands

CMD	Description	Change	Comments
0	Read Unique Identifier	(♦)	
1	Read Primary Variable		
2	Read Loop Current and Percent of Range		
3	Read Dynamic Variables and Loop Current		
6	Write Polling Address		
7	Read Loop Configuration		
8	Read Dynamic Variable Classifications		
9	Read Device Variables with Status		
11	Read Unique Identifier Associated With Tag	(♦)	
12	Read Message		
13	Read Tag, Descriptor, Date		
14	Read Primary Variable Transducer Information		
15	Read Device Information		
16	Read Final Assembly Number		
17	Write Message		
18	Write Tag, Descriptor, Date		
19	Write Final Assembly Number		
20	Read Long Tag		
21	Read Unique Identifier Associated With Long Tag	(♦)	
22	Write Long Tag		
38	Reset Configuration Changed Flag		
48	Read Additional Device Status	(♦)	

5.2 Common Practice Commands

CMD	Description	Change	Comments
41	Perform device self-test		
42	Perform device reset		
59	Write number of response preambles		
71	Lock Device		
73	Find Device		
74	Read I/O system capabilities		
75	**Poll Sub-Device**	(●)	Already supported but not document in latest previous release.
76	Read Lock Device State		
77	Send CMD to sub-device using card/channel		
78	Read Aggregated Commands		
84	Read sub-device identity summary using list index		
85	Read I/O channel statistics using card/channel		
86	Read sub-device statistics using list index		
87	Write I/O System Master Mode		
88	Write I/O System Retry Count		
89	Set real-time clock		
90	Read real-time clock		
94	Read I/O system host statistics		
106	Flush delayed response buffers		
512	Read country code		
513	Write country code		

5.3 Wireless Commands

CMD	Description	Change	Comments
768	Modify Common Join Key	(♦)	
773	Write Network Id		
774	Read Network Id		
775	Write Network Tag		
776	Read Network Tag		
794	Read UTC time mapping		
797	Write Radio Power		
798	Read Radio Power		
814	Read Device List entries using list index	(♦)	
815	**Add Device List Table Entry**	(●)	Always return “invalid selection”.
816	Delete Device List entry using unique ID	(♦)	
817	Read RF Channel Blacklist		
817	Write RF Channel Blacklist		
821	Write Network Access Mode	(♦)	
822	Read network Access Mode	(♦)	
832	Read Device Nickname & Long Tag Using Unique ID		
835	Read Network Device burst mode list using unique ID		
836	Flush device cached responses using unique ID		
840	Read Network Device Statistics		
841	Read Network Device Identity & Long Tag Using Nickname		
842	Write Network Device Scheduling Flags		
843	Read Network Device Scheduling Flags		
848	**Generate Key**	(●)	

5.4 Device Specific Commands

CMD	Description	Change	Comments
122	Write Device ID		Non-public command.
123	Write Expanded Device Type Code		Non-public command.
124	Write Manufacturer Identification Code		Non-public command.
125	Write Private Label Distributor Code		Non-public command.
126	Write PFDCP Information		Non-public EtherNetIP command.
127	Reserved command number		Not to be used.
128	Get Special Operating Mode	(♦)	
129	Set Special Operating Mode	(♦)	
130	Cache-bypass CMD 77 version		
131	Flush Device DR buffers using unique ID		
132	Read Device List Entries with “status-mask”		
133	Read Active Serial Protocol		
134	Write Active Serial Protocol		
135	Read HART Communication Parameters		
136	Write HART Communication Parameters		
139	Read TCP/IP Parameters		
140	Write TCP/IP Parameters		
141	Perform Reset Action		
142	Read “shadow-list” element		
143	Write “shadow-list” element		
144	Read latest CMD 3 response		
145	Read sub-device identity & status	(♦)	
146	Set Fast Pipe Status		
147	Verify Fast Pipe Status		
148	Read sub-device identity & status & MAC	(♦)	
149	**Abort Joinkey Change Procedure**	(●)	
152	Enable Global Advertising		
153	Restore Default Values		
154	Force Device Identification		
155	Read Ethernet MAC Address		
156	Write XML Protocol Port		
157	Read XML Protocol Port		
158	Set Bandwidth Profile		
159	Verify Bandwidth Profile		
160	Set Logging Mode		
161	Verify Logging Mode		

CMD	Description	Change	Comments
164	**Start Joinkey Change Procedure**	**(•)**	
165	Set Holding Registers Reroute Mode		
166	Verify Holding Registers Reroute Mode		
170	Get Network Statistics		
171	Get Device Statistics		
172	Get Path Statistics		
173	Get Cached Device Statistics		
174	Get Cached Paths Statistics		
175	Get Cached Device Parameters		
176	Read Device Coordinates		
177	Write Device Coordinates		
178	Write Gateway CIP parameters		EtherNET-IP command
179-180	----------		Free for future usage
181	Read Adapter List		EtherNET-IP command
182	Read Aggregated Wireless Information		EtherNET-IP command
183	**Verify Discrete Device Downstream Period**	(•)	
184	**Set Discrete Device Downstream Period**	(•)	
185	**Transfer to Whitelist**	(•)	
186	**Read Device Time-Stamp Info**	(•)	
187	**Temporary Join Mode Control**	(•)	
188	**Set Dynamic Variables Stale Thresholds**	(•)	
189	**Verify Dynamic Variables Stale Thresholds**	(•)	
190	**Set Device DV Substitution Values**	(•)	
191	**Verify Device DV Substitution Values**	(•)	
192	**Verify Key Change Progress**	(•)	
193-225	----------		Free for future usage
226	Read software version		ENP command
227	Read serial number		ENP command
228	Read order code		ENP command
229	Write serial number		ENP command
230	Write order code		ENP command
231	Check device status		ENP command
232	Write service code		ENP command
233	Read order Identifier		ENP command
234	Read ENP version		ENP command
235	Write order Identifier		ENP command
236-255	----------		Free for future usage

6. DOCUMENT RELEASE NOTES

Document first released along with Gateway ***Revision 3.0*** (this document supersedes *GatewayCommandsSummaryR16*)

- **R0 – 11/04/2016**

  First document release.

- **R1 – 11/04/2018**

  Release 03.00.07: “Improved the procedure used to establish the session with the Network Manager, in order to cope with variable booting time after the device has been powered-up”

- **R2 – 05/03/2019**

  Release 03.00.08: Improved the interaction between master operations performed by the gateway itself and the external HART masters. Bug fixing.