



OPERATION INSTRUCTIONS

OMDxxx-R2000

Ethernet communication protocol

Protocol version 1.02





Contents

1 Protocol basics	5
1.1 Basic design	5
1.2 HTTP command protocol	5
1.2.1 Sending commands	6
1.2.2 Query argument encoding	6
1.2.3 Replies to commands	6
1.2.4 HTTP request and reply – low level example	7
1.2.5 HTTP status codes	7
1.2.6 Sensor error codes	8
1.2.7 Protocol information (<code>get_protocol_info</code>)	8
2 Sensor parametrization using HTTP	10
2.1 Parameter types	10
2.1.1 Enumeration values (<code>enum</code>)	10
2.1.2 Boolean values (<code>bool</code>)	10
2.1.3 Bit fields (<code>bitfield</code>)	11
2.1.4 Integer values (<code>int, uint</code>)	11
2.1.5 Double values (<code>double</code>)	11
2.1.6 String values (<code>string</code>)	11
2.1.7 IPv4 address and network mask values (<code>IPv4</code>)	12
2.1.8 NTP timestamp values (<code>ntp64</code>)	12
2.1.9 Binary data (<code>binary</code>)	12
2.2 Commands for sensor parametrization	13
2.2.1 <code>list_parameters</code> – list parameters	13
2.2.2 <code>get_parameter</code> – read a parameter	13
2.2.3 <code>set_parameter</code> – change a parameter	14
2.2.4 <code>reset_parameter</code> – reset a parameter to its default value	14
2.2.5 <code>reboot_device</code> – restart the sensor firmware	15
2.2.6 <code>factory_reset</code> – reset the sensor to factory settings	15
2.3 Basic sensor information	17
2.3.1 Parameter overview	17
2.3.2 Device family (<code>device_family</code>)	17
2.3.3 User defined strings (<code>user_tag, user_notes</code>)	17
2.4 Sensor capabilities	18
2.4.1 Parameter overview	18
2.4.2 Device features (<code>feature_flags</code>)	18
2.4.3 Emitter type (<code>emitter_type</code>)	18
2.5 Ethernet configuration	19
2.5.1 Parameter overview	19
2.5.2 IP address mode (<code>ip_mode</code>)	19
2.6 Measuring configuration	20
2.6.1 Parameter overview	20
2.6.2 Mode of operation (<code>operating_mode</code>)	20
2.6.3 Scan frequency (<code>scan_frequency, scan_frequency_measured</code>)	20
2.6.4 Scan direction (<code>scan_direction</code>)	21
2.6.5 Scan resolution (<code>samples_per_scan</code>)	21
2.7 HMI / Display configuration	22
2.7.1 Parameter overview	22
2.7.2 HMI display mode (<code>hmi_display_mode</code>)	23
2.7.3 HMI display language (<code>hmi_language</code>)	23
2.7.4 HMI button lock (<code>hmi_button_lock</code>)	23
2.7.5 HMI parameter lock (<code>hmi_parameter_lock</code>)	23
2.7.6 Locator indication (<code>locator_indication</code>)	23
2.8 System status	24
2.8.1 Parameter overview	24
2.8.2 System status flags (<code>status_flags</code>)	24
2.8.3 System load indication (<code>load_indication</code>)	25



3 Scan data output using TCP or UDP	26
3.1 Principles of scan data acquisition	26
3.1.1 Sensor coordinate system	26
3.1.2 Scan data coordinate system	27
3.1.3 Distance readings	27
3.1.4 Echo amplitude readings	27
3.1.5 Timestamps	28
3.2 Principles of scan data output	29
3.2.1 Introduction	29
3.2.2 Scan data connection handles	29
3.2.3 Scan data connection watchdog	30
3.2.4 Scan data output customization	30
3.2.5 Using multiple concurrent scan data connections	31
3.3 Commands for managing scan data output	32
3.3.1 request_handle_udp – request for an UDP-based scan data channel	32
3.3.2 request_handle_tcp – request for a TCP-based scan data channel	33
3.3.3 release_handle – release a data channel handle	35
3.3.4 start_scanoutput – initiate output of scan data	35
3.3.5 stop_scanoutput – terminate output of scan data	35
3.3.6 set_scanoutput_config – reconfigure scan data output	36
3.3.7 get_scanoutput_config – read scan data output configuration	37
3.3.8 feed_watchdog – feed connection watchdog	37
3.3.9 TCP in-line watchdog feeds	38
3.4 Transmission of scan data	39
3.4.1 Basic packet structure	39
3.4.2 Typical structure of a scan data header	40
3.4.3 Scan data header status flags	41
3.4.4 Scan data packet type A – distance only	42
3.4.5 Scan data packet type B – distance and amplitude	43
3.4.6 Scan data packet type C – distance and amplitude (compact)	44
3.5 Data transmission using TCP	45
3.6 Data transmission using UDP	45
4 Working with the HMI LED display	46
4.1 Technical overview	46
4.2 Displaying custom text messages	47
4.2.1 Overview	47
4.2.2 Static text messages (static text)	47
4.2.3 Dynamic text messages (application text)	48
4.3 Displaying custom bitmaps	48
4.3.1 Overview	48
4.3.2 Static bitmaps	49
4.3.3 Application bitmaps	49
4.3.4 Converting graphics for the HMI display	49
5 Advanced topics	51
5.1 Device discovery using SSDP	51
5.1.1 SSDP search request	51
5.1.2 SSDP device reply	51
5.1.3 SSDP device description	52
A Troubleshooting the Ethernet communication	53
A.1 Checking the Ethernet setup	53
A.2 Debugging using a web browser	53
A.3 Debugging using Wireshark	53
B Protocol version history	55
B.1 Protocol version 1.02 (R2000 firmware v1.21 or newer)	55
B.2 Protocol version 1.01 (R2000 firmware v1.20 or newer)	55
B.3 Protocol version 1.00 (R2000 firmware v1.00 or newer)	55
C Document change history	56
C.1 Release 2016-03 (protocol version 1.02)	56
C.2 Release 2015-04 (protocol version 1.01)	56
C.3 Release 2013-08 (protocol version 1.00)	56



Index for commands and parameters	57
References	58



1 Protocol basics

This chapter describes the basics of the Pepperl+Fuchs scan data protocol (PFSDP).

1.1 Basic design

The communication protocol specification is based on the following basic design decisions:

- A simple command protocol using HTTP requests (and responses) is provided in order to parametrize and control the sensor. The HTTP can be accessed using a standard web browser or by establishing temporary TCP/IP connections to the HTTP port.
- Sensor process data (scan data) is received from the sensor using a separate TCP/IP or UDP/IP channel. A TCP channel is recommended for every application that requires a secure and error proof transmission of scan data. An UDP channel is recommended for applications in need of minimum latency transmission of scan data.

Output of scan data is always conform to the following conventions:

- Data output is performed as packets with a packet size adapted to the common Ethernet frame size (TCP as well as UDP).
- A single packet always contains data of a single continuous scan only. Scan data output always starts with a new packet for every (new) scan.
- For scan data output the user application can select from multiple data types with different levels of information detail. This way a client can decide to receive only the amount of data needed for its individual application – reducing traffic. Furthermore this provides an easy way to implement future extensions to the scan data output (e.g. adding additional information) as well.
- The byte order for all binary data is *LittleEndian* (least significant byte first). The DSP of the sensor and PC CPUs both use LittleEndian – thus no conversions need to take place.
- The sensor does not strictly restrict neither the number of active client connections nor the amount of (scan) data requested by clients. Basically it is the users responsibility to design his (client) system or application in a way that the sensor can handle the amount of requested data without getting overloaded.

1.2 HTTP command protocol

The HTTP command protocol provides a simple unified way to control sensor operation for application software. HTTP commands are used to configure sensor measurement as well as to read and change sensor parameters. Furthermore it can be used to set up (parallel) TCP or UDP data channels providing sensor scan data.

This section describes the basic HTTP command protocol and various commands available to the user. Transmission of scan data using an additional TCP or UDP channel is explained in section 3.4.

Please note:

The R2000 provides full support for HTTP/1.1 – but does currently not support persistent connections (which is optional according to the HTTP/1.1 standard [4]). Each HTTP response includes the "Connection: close" header to inform the client that a subsequent HTTP request requires a separate TCP/IP connection to the sensor.



1.2.1 Sending commands

Sending commands to the sensor is done using the Hypertext Transfer Protocol (HTTP) as defined by RFC 2616 [4]. Each HTTP command is constructed as **Uniform Resource Identifier (URI)** according to RFC 3986 [7] with the following basic structure:

```
<scheme>:<authority>/<path>?<query>#<fragment>
```

A typical HTTP request to the sensor looks like:

```
http://<sensor IP address>/cmd/<cmd_name>?<argument1=value>&<argument2=value>
```

Thus, in terms of an URI a valid HTTP command is composed of the following parts:

- **scheme** is always 'http://'
- **authority** is represented by the IP address of the sensor (and a port number, if necessary)
- **path** consists of the prefix 'cmd/' and the name of the requested command ('<cmd_name>')
- **query** lists additional arguments for the specific command
- **fragment** is currently not used – anything following the hash mark will be ignored

Please note:

The order of the command arguments (within <query>) is interchangeable at will. Sole exception is the argument `handle` (see section 3.3), which has to be specified always first in order to identify the client scan data connection – provided that this is required for the requested command.

Please note:

The number of command arguments (within <query>) is limited to 100. Furthermore, the maximum length of a HTTP request URI is limited to 16 kB. Typical user application do not exceed these limitation, though.

1.2.2 Query argument encoding

The query part of the command URI (see section 1.2.1) is used to transport additional arguments to HTTP commands (compliant to RFC 3986 [7]). This section describes the composition of arguments as "key=value" pairs.

HTTP command arguments are composed using the following scheme ("key=value" pairs):

```
key=value[;value][&key=value]
```

The `key` denotes an argument that receives one or more values. Multiple values for a single argument are separated by a semi-colon ';'. A single command takes multiple arguments separated by an ampersand '&'.

Please note:

Some characters are reserved within an URI and need to be percent encoded according to the rules of RFC 3986 [7]. Most notably, if parameter values contain URI delimiters like the question mark '?', equal sign '=' or the ampersand '&', these characters need to be escaped on the URI.

1.2.3 Replies to commands

After sending a command to the sensor the following replies can be received:

- **HTTP status code**

A HTTP command will be answered with a standard HTTP status code first. This code indicates whether the command (i.e. URI) is known and has been received correctly. An error code is returned only if the URI is invalid or could not be processed. Please refer to section 1.2.5 for a detailed description of HTTP status codes used by the R2000.

- **Command error code**

Normally the HTTP status code is read as 'OK'. In this case the result of the command processing can be evaluated using two return values: `error_code` and `error_text`. `error_code` contains a numeric result code for the command call, while `error_text` provides a textual error description. Both values are returned using **JSON encoding** [9]. Section 1.2.6 provides a detailed description of all R2000 command error codes.

- **Command reply data**

The body of a command reply contains any requested payload data. This data is always transmitted using **JSON encoding** [9]. Large amounts of data might be output using `base64` encoded JSON arrays.

**Please note:**

The character encoding used for all JSON encoded command replies of the R2000 is always UTF-8 (RFC 7159 [9]).

1.2.4 HTTP request and reply – low level example

This section shows an example, how a HTTP request is transmitted to the sensor without using a web-browser. Lets assume, that the following HTTP request shall be send:

```
http://<sensor IP address>/cmd/get_parameter?list=scan_frequency
```

This request is translated into a simple string (using HTTP/1.0 in this example):

```
1 GET /cmd/get_parameter?list=scan_frequency HTTP/1.0\r\n\r\n
```

This string is then send as payload data of a TCP/IP packet to the sensor. The sensor then sends back a TCP/IP packet with the HTTP reply as payload data. The HTTP reply can be parsed as simple text string with the following content:

```
1 HTTP/1.0 200 OK\r\n
2 Expires: -1\r\n
3 Pragma: no-cache\r\n
4 Content-Type: text/plain\r\n
5 Connection: close\r\n
6 \r\n
7 f\r\n
8 "scan_frequency":50,\r\n
9 "error_code":0,\r\n
10 "error_text":"success"\r\n
11 }\r\n
```

The most important parts of this HTTP reply are the first line containing the HTTP error code and the last few lines containing the requested information wrapped within a single **JSON-encoded** [9] object denoted by a pair of curly brackets.

Please note:

It is highly recommended to use a third party HTTP library instead of a new custom implementation. Standards-compliant HTTP client implementations are widely available for most operation systems and hardware platforms (e.g. Libwww [10] or libcurl [11]).

1.2.5 HTTP status codes

The following table lists all **HTTP status codes** used by the device:

status code	message	description
200	OK	request successfully received
400	Bad Request	wrong URI syntax
403	Forbidden	permission denied for this URI
404	Not Found	unknown command code or unknown URI
405	Method not allowed	invalid method requested (currently only GET is allowed)

Examples for (invalid) queries causing a HTTP error

request	status code	error message
http://<ip>/cmd/nonsense	400	"unrecognized command"
http://<ip>/cmd/get_parameter&test	400	"unrecognized command"
http://<ip>/cmd/get_parameter?list	400	"parameter without value"
http://<ip>/test	404	"file not found"
http://<ip>/test/	404	"file not found"
http://<ip>/test/file	404	"file not found"

1.2.6 Sensor error codes

The following table lists some generic error codes (`error_code`) returned by the device:

error code	description (error_text)
0	"success"
100	"unknown argument '%s'"
110	"unknown parameter '%s'"
120	"invalid handle or no handle provided"
130	"required argument '%s' missing"
200	"invalid value '%s' for argument '%s'"
210	"value '%s' for parameter '%s' out of range"
220	"write-access to read-only parameter '%s'"
230	"insufficient memory"
240	"resource already/still in use"
333	"(internal) error while processing command '%s'"

Examples for (invalid) commands provoking sensor error codes

command (query)	code	error message
/cmd/get_protocol_info?list=test	100	"Unknown argument 'list'"
/cmd/get_parameter?list=test	110	"Unknown parameter 'test'"
/cmd/start_scanoutput	120	"Invalid handle or no handle provided"
/cmd/start_scanoutput?handle=test	120	"Invalid handle or no handle provided"
/cmd/set_parameter?ip_address=777	200	"Invalid value '777' for argument 'ip_address'."
/cmd/set_parameter?scan_frequency=999	210	"Value '999' for parameter 'scan_frequency' is out of range."
/cmd/set_parameter?serial=123456	220	"Write-access to read-only parameter 'serial'"

1.2.7 Protocol information (get_protocol_info)

Ethernet protocol users should be aware that depending on the protocol version some commands might not be available or might show different behavior. For this reason user applications should always check the protocol version using the dedicated command `get_protocol_info` which returns basic version information on the communication protocol:

parameter name	type	description
protocol_name	string	Protocol name (currently always 'pfSdP')
version_major	uint	Protocol major version (e.g. 1 for 'v1.02', 3 for 'v3.10')
version_minor	uint	Protocol minor version (e.g. 2 for 'v1.02', 10 for 'v3.10')
command_list	string	List of all available HTTP commands

This document refers to protocol version '1.02' which is implemented by R2000 firmware version 1.21 and newer.

Please note:

The command `get_protocol_info` will return the above information on every sensor – regardless of its firmware version. All other commands and their return values might be changed by updates to the communication protocol, though. Therefore it is strongly recommended to check the protocol version first.

Example

Query: `http://<sensor IP address>/cmd/get_protocol_info`



Reply: {

```
"protocol_name":"pfpsdp",
"version_major":1,
"version_minor":1,
"commands":[
    "get_protocol_info",
    "list_parameters",
    "get_parameter",
    "set_parameter",
    "reboot_device",
    "reset_parameter",
    "request_handle_udp",
    "request_handle_tcp",
    "feed_watchdog",
    "get_scanoutput_config",
    "set_scanoutput_config",
    "start_scanoutput",
    "stop_scanoutput",
    "release_handle"
],
"error_code":0,
"error_text":"success"
}
```



2 Sensor parametrization using HTTP

2.1 Parameter types

The sensor provides access to different types of parameters. The following table gives a quick overview of the relevant types, a more detailed description follows in separate sub-sections:

type	description
enum	enumeration type with a set of named values (strings)
bool	boolean values (on / off)
bitfield	a set of boolean flags
int	signed integer values
uint	unsigned integer values
double	floating point values with double precision
string	strings composed of UTF-8 characters
ipv4	Internet Protocol version 4 addresses or network masks
ntp64	NTP timestamp values
binary	Binary data

Independently of their type, each parameter belongs to one of the following access groups:

access	description
sRO	static Read-Only access (value never changes)
RO	Read-Only access (value might change during operation)
RW	Read-Write access (non-volatile storage)
vRW	volatile Read-Write access (lost on reset)

Most sensor parameters are stored into non-volatile memory. Thus their value persists even if the device encounters a power-cycle. Please note though, that non-volatile storage has a limited number of write cycles only (typical > 10.000 cycles). Therefore all non-volatile parameters should be written only if necessary.

2.1.1 Enumeration values (enum)

Notes on parameters using enumeration values (enum):

- An enumeration type parameter accepts a single value out of a list of predefined values.
- Each enumeration values is defined by a string ('named' value).
- Each enumeration value is typically (but not necessarily) unique to the specific parameter.
- Each enum parameter can hold only a single value at a time.
- URI: Named enumeration values use non-reserved ASCII characters only and need no percent encoding [7] when specified as argument to a command on the URI.

2.1.2 Boolean values (bool)

Notes on parameters using boolean values (bool):

- Boolean parameters are a special case of enumeration parameters.
- Only the named values on and off are accepted.
- Each bool parameter can hold only a single value at a time.



2.1.3 Bit fields (bitfield)

Notes on parameters using bit fields (`bitfield`):

- Bit fields combine multiple boolean flags into an unsigned integer value.
- Each flag occupies a single bit of the integer.
- Not every bit of the integer needs to be assigned to a flag.
- Bits might be marked as *reserved*. These should always be zero.
- Bit field parameters are read and written using the integer representation.

2.1.4 Integer values (int, uint)

Notes on parameters using signed integer values (`int`) and unsigned integer value (`uint`):

- Unless denoted differently, the value range of integer values is limited to 32 bit.
- Leading zeros are accepted when writing a value (they will be ignored).
- Neither a hexadecimal nor an octal representation of integer values is supported.

2.1.5 Double values (double)

Notes on parameters using double precision floating point values (`double`):

- A dot '.' is used as decimal mark (separating the decimal part from the fractional part of a `double` number).
- The floating point decimal format (xxx.yyy) should be used when accessing `double` parameters. The floating point exponential format (xxx.yyy Ezzz) is not supported.
- The number of significant digits of the fractional part of a `double` value might be limited for some parameters. Excess digits are rounded or discarded.

2.1.6 String values (string)

Notes on parameters using string values (`string`):

- Strings represent a set characters.
- All characters of the string need to be encoded in UTF-8 format [6].
- The maximum size of a string is usually limited. Please refer to the description of the specific parameter for its actual size limitation.
- URI: For write access to a `string` parameter, its new value is implicitly delimited by the surrounding '=' and '&' within the URI (see RFC 3986 [7]). Any additionally added delimiter (e.g. '') will be interpreted as part of the string.
- URI: Some characters are reserved within an URI and need to be percent encoded [7] (see section 1.2.2 for details).

When parsing a `string`-typed parameter within an UTF-8 encoded command URI the sensor performs the following steps:

1. Dissect the URI into its individual parts
2. Resolve percent encoded characters
3. Check string for a valid UTF-8 encoding
4. Process the string (UTF-8 bytes), e.g. store it into non-volatile memory

When the sensor outputs a `string`-typed parameter in JSON format, it applies escaping for the following reserved UTF-8 characters (as required by RFC 7159 [9] section 2.5):

character	code	replacement
backspace	U+0008	'\b'
tabulator	U+0009	'\t'
new line	U+000A	'\n'
form feed	U+000C	'\f'
carriage return	U+000D	'\r'
double quote	U+0022	'\"'
solidus	U+002F	currently not replaced
backslash	U+005C	'\\'
other control characters	U+0000 ... U+001F	'\uXXXX'

2.1.7 IPv4 address and network mask values (IPv4)

Notes on parameters using IPv4 network addresses and subnet masks (IPv4):

- Addresses and network masks need to follow the rules of the Internet Protocol specification (RFC-791 [1])
- Addresses are denoted as `string` values in human-readable *dotted decimal* notation (i.e. 10.0.10.9)
- Subnet masks are denoted as `string` values in human-readable *dotted decimal* notation (i.e. 255.255.0.0)

2.1.8 NTP timestamp values (ntp64)

Notes on parameters using NTP timestamps (ntp64):

- NTP timestamps are part of the Network Time Protocol (NTP) as defined by RFC 1305 [2].
- NTP timestamps are represented as a 64 bit unsigned fixed-point integer number (`uint64`) in seconds in reference to a specific point in time. The most significant 32 bit represent the integer part (seconds), the lower 32 bit the fractional part.
- *Absolute* timestamps (synchronized time) refer to the time elapsed since 1 January 1900.
- *Relative* timestamps (raw system time) refer to the time elapsed since power-on of the sensor.

Please refer to section 3.1.5 for more details on timestamps.

2.1.9 Binary data (binary)

Notes on parameters using binary data (binary):

- Parameters of type `binary` store binary data without further data-specific knowledge. Parameter values are simply treated as a collection of bytes. The interpretation of binary data is specific to the individual parameter. See the description of the specific parameter for details.
- For binary parameters usually only size checking is performed. The maximum size of data depends on the specific parameter.
- Read access to a `binary` parameter returns its value as `base64` encoded string within the JSON reply (see section 1.2.3). The `base64` encoding transforms an 8 bit data stream to a string with a particular set of 64 ASCII characters (6 bit) that are printable and common to most character encodings (see RFC 4648 [8] for details). This encoding requires 33 % more storage space.
- Write access to a `binary` parameter requires the binary data to be encoded as `base64url` [8] string on the URI. The `base64url` encoding is very similar to the `base64` encoding but uses a slightly different character set, that avoids using reserved URI characters.



2.2 Commands for sensor parametrization

This section describes all commands available for manipulation of global sensor parameters.

2.2.1 list_parameters – list parameters

The command `list_parameters` returns a list of all available global sensor parameters.

Example

Query: `http://<sensor IP address>/cmd/list_parameters`

Reply:

```
{  
    "parameters": [  
        "vendor",  
        "product",  
        "part",  
        "serial",  
        "revision_fw",  
        "revision_hw",  
        "max_connections",  
        "feature_flags",  
        "radial_range_min",  
        "radial_range_max",  
        "radial_resolution",  
        "angular_fov",  
        "angular_resolution",  
        "ip_mode",  
        "ip_address",  
        "subnet_mask",  
        "gateway",  
        "scan_frequency",  
        "scan_direction",  
        "samples_per_scan",  
        "scan_frequency_measured",  
        "status_flags",  
        "load_indication",  
        "device_family",  
        "mac_address",  
        "hmi_display_mode",  
        "hmi_language",  
        "hmi_button_lock",  
        "hmi_parameter_lock",  
        "ip_mode_current",  
        "ip_address_current",  
        "subnet_mask_current",  
        "gateway_current",  
        "system_time_raw",  
        "user_tag",  
        "user_notes",  
        "locator_indication",  
    ],  
    "error_code": 0,  
    "error_text": "success"  
}
```

2.2.2 get_parameter – read a parameter

The command `get_parameter` reads the current value of one or more global sensor parameters:

```
http://<sensor IP address>/cmd/get_parameter?list=<param1>;<param2>
```

Command arguments

- `list` – semicolon separated list of parameter names (optional)

If the argument `list` is not specified the command will return the current value of all available parameters.

Example

Query: `http://<sensor IP address>/cmd/get_parameter?list=scan_frequency;scan_frequency_measured`

Reply: {

```
"scan_frequency":50,  
"scan_frequency_measured":49.900000,  
"error_code":0,  
"error_text":"success"  
}
```

2.2.3 set_parameter – change a parameter

Using the command `set_parameter` the value of any write-accessible global sensor parameter can be changed:

`http://<sensor IP address>/cmd/set_parameter?<param1>=<value>&<param2>=<value>`

Command arguments

- `<param1> = <value>` – new `<value>` for parameter `<param1>`
- `<param2> = <value>` – new `<value>` for parameter `<param2>`
- ...

Please note:

The command `set_parameter` returns an error message, if any parameter specified as command argument is unknown or a read-only parameter. The return values `error_code` and `error_text` have appropriate values in this case (see section 1.2.6).

Example

Query: `http://<sensor IP address>/cmd/set_parameter?scan_frequency=50`

Reply: {

```
"error_code":0,  
"error_text":"success"  
}
```

2.2.4 reset_parameter – reset a parameter to its default value

The command `reset_parameter` resets one or more global sensor parameters to their factory default values:

`http://<sensor IP address>/cmd/reset_parameter?list=<param1>;<param2>`

Command arguments

- list – semicolon separated list of parameter names (optional)

Please note:

If the argument list is not specified the command will load the factory default value for all parameters writeable with set_parameter!

Please note:

This command applies to global R/W parameters accessible via the command set_parameter only. If the argument list contains an unknown or a read only parameter, an error message will be returned.

Please note:

Resetting a parameter to its default value might require a device restart in order to take effect. For example, this applies to all Ethernet configuration parameters (see section 2.5).

Example

Query: `http://<sensor IP address>/cmd/reset_parameter?list=scan_frequency;scan_direction`

Reply: {

```
"error_code":0,  
"error_text":"success"  
}
```

2.2.5 reboot_device – restart the sensor firmware

The command reboot_device triggers a soft reboot of the sensor firmware:

`http://<sensor IP address>/cmd/reboot_device`

Command arguments

The command accepts no additional arguments. The reboot is performed shortly after the HTTP reply has been sent.

Please note:

A reboot terminates all running scan data output. All scan data handles are invalidated and have to be renewed from scratch after reboot (see section 3.4).

Please note:

A device reboot takes up to 60 s (depending on the sensor configuration). The reboot is completed as soon as the sensor answers to HTTP command requests again and the system status flag *Initialization* (see section 2.8.2) is cleared.

Example

Query: `http://<sensor IP address>/cmd/reboot_device`

Reply: {

```
"error_code":0,  
"error_text":"success"  
}
```

2.2.6 factory_reset – reset the sensor to factory settings

Protocol version 1.01 adds the command factory_reset that performs a complete reset of all sensor settings to factory defaults and reboots the device. Its result is similar to a call of reset_parameter without any arguments followed by a call to reboot_device.

Command arguments

The command accepts no additional arguments. The factory reset and device reboot is performed shortly after the HTTP reply has been sent.

Please note:

The factory reset performs a device reboot, because some changes take effect at sensor boot time only (e.g. all changes to Ethernet configuration parameters – see section 2.5).

Example

Query: `http://<sensor IP address>/cmd/factory_reset`

Reply: {

```
  "error_code":0,  
  "error_text":"success"  
}
```



2.3 Basic sensor information

This section describes all sensor parameters which are available to the user.

2.3.1 Parameter overview

The following table lists numerous parameters (mostly read-only) which provide basic sensor information:

parameter name	type	description	access
device_family	uint	Numeric unique identifier (see below)	sRO
vendor	string	Vendor name (max. 100 chars)	sRO
product	string	Product name (max. 100 chars)	sRO
part	string	Part number (max. 32 chars)	sRO
serial	string	Serial number (max. 32 chars)	sRO
revision_fw	string	Firmware revision (max. 32 chars)	sRO
revision_hw	string	Hardware revision (max. 32 chars)	sRO
user_tag	string	User defined name (max. 32 chars)	RW
user_notes	string	User notes (max. 1000 Byte)	RW

These entries are comparable to generic information available on IO-Link devices. In contrast to IO-Link most strings have no size limitation, though. Furthermore each parameter can be read individually using the command `get_parameter`.

2.3.2 Device family (device_family)

The parameter `device_family` can be used to identify compatible device families. A single device family is defined as group of devices with identical functionality (regarding the Ethernet protocol). This identifier can be used to check if the connected device is compatible with the client application (e.g. DTM user interface).

Currently the following values are defined for `device_family`:

value	description
0	reserved
1	OMDxxx-R2000 (UHD raw data devices)
2	reserved
3	OMDxxx-R2000-HD (HD raw data devices)

2.3.3 User defined strings (user_tag, user_notes)

The parameters `user_tag` and `user_notes` are strings, that can be used by the user without restriction (except for a valid UTF-8 encoding – see definition of type `string` in section 2.1). The default value for `user_tag` is typically a short version of the product name (parameter `product`) while `user_notes` is empty per default.



2.4 Sensor capabilities

2.4.1 Parameter overview

The following static read-only parameters describe the sensor capabilities:

parameter name	type	unit	description	access
feature_flags	array		sensor feature flags (see below)	sRO
emitter_type	uint		type of light emitter used by the sensor (see below)	sRO
radial_range_min	double	m	min. measuring range (distance)	sRO
radial_range_max	double	m	max. measuring range (distance)	sRO
radial_resolution	double	m	max. radial resolution (distance)	sRO
angular_fov	double	°	max. angular field of view	sRO
angular_resolution	double	°	max. angular resolution	sRO
scan_frequency_min	uint	Hz	min. supported scan frequency (see section 2.6)	sRO
scan_frequency_max	uint	Hz	max. supported scan frequency (see section 2.6)	sRO
sampling_rate_min	uint	Hz	min. supported sampling rate (see section 2.6)	sRO
sampling_rate_max	uint	Hz	max. supported sampling rate (see section 2.6)	sRO
max_connections	uint		max. number of concurrent scan data channels (connections)	sRO
max_scan_sectors	uint		max. number of scan sectors (0 if not supported)	sRO
max_data_regions	uint		max. number of data regions (per scan data channel)	sRO

2.4.2 Device features (feature_flags)

The parameter `feature_flags` returns a JSON [9] encoded list of features available for the queried device. Currently the following features are defined:

feature name	description	reference
ethernet	Ethernet interface	

If a feature is available, its name is listed within the `feature_flags` array.

2.4.3 Emitter type (emitter_type)

The parameter `emitter_type` can be used to determine the type of light emitter (aka `transmitter`) used by the specific sensor. Currently the following emitter types are defined for R2000 devices:

type	description
0	undefined / reserved
1	red laser (660 nm)
2	infrared laser (905 nm)



2.5 Ethernet configuration

2.5.1 Parameter overview

The following parameters allow configuration changes of the Ethernet interface:

parameter	type	description	access	default
ip_mode	enum	IP address mode: static, dhcp, autoip	RW	static
ip_address	ipv4	static IP mode: sensor IP address	RW	10.0.10.9
subnet_mask	ipv4	static IP mode: subnet mask	RW	255.255.255.0
gateway	ipv4	static IP mode: gateway address	RW	0.0.0.0
ip_mode_current	enum	current IP address mode: static, dhcp, autoip	RO	static
ip_address_current	ipv4	current sensor IP address	RO	10.0.10.9
subnet_mask_current	ipv4	current subnet mask	RO	255.255.255.0
gateway_current	ipv4	current gateway address	RO	0.0.0.0
mac_address	string	sensor MAC address (00-0D-81-xx-xx-xx)	RO	-

The read-only parameters `ip_mode_current`, `ip_address_current`, `subnet_mask_current` and `gateway_current` provide access to the currently active IP configuration. This is especially useful when using automatic IP configuration via DHCP or AutoIP.

Please note:

Any changes to the Ethernet configuration (using `set_parameter` or `reset_parameter`) are applied after a system reboot only! The command `reboot_device` (see section 2.2.5) is available to initiate a reboot using the Ethernet protocol.

2.5.2 IP address mode (`ip_mode`)

The parameter `ip_mode` configures one of the following IP address modes:

- `static` – static IP configuration using `ip_address`, `subnet_mask`, `gateway`
- `autoip` – automatic IP configuration using "Zero Configuration Networking" [14]
- `dhcp` – automatic IP configuration using a DHCP server

Please note:

With automatic IP configuration using DHCP or AutoIP the parameters `ip_address_current` and `subnet_mask_current` might return the invalid IP address 0.0.0.0 if no valid IP address has been assigned to the sensor yet (e.g. if no DHCP server is found).

2.6 Measuring configuration

2.6.1 Parameter overview

The following (global) parameters are available for basic measurement configuration:

parameter name	type	unit	description	access	default
operating_mode	enum	—	mode of operation: measure, transmitter_off	vRW	measure
scan_frequency	double	1 Hz	scan frequency (10 Hz..50 Hz)	RW	35 Hz
scan_direction	enum	—	direction of rotation: cw or ccw	RW	ccw
samples_per_scan	uint	samples	number of readings per scan	RW	3600
scan_frequency_measured	double	1 Hz	measured scan frequency	RO	—

2.6.2 Mode of operation (operating_mode)

The parameter `operating_mode` controls the mode of operation of the sensor. Currently, the following modes are available:

parameter name	description
<code>measure</code>	Sensor is recording scan data
<code>transmitter_off</code>	Emitter is disabled, no scan data is recorded

The mode `measure` is the normal mode of operation of the sensor and default after power-on. The mode `transmitter_off` allows the user to deactivate the light emitter, e.g. to avoid interference with other optical devices. A mode switch from `measure` to `transmitter_off` can only be performed, if no scan data connections are active, i.e. all handles have been released. While the operating mode is set to `transmitter_off`, no new scan data connection handles can be requested (see section 3.2). This state is also signaled by the system status flag `scan_output-muted` (see section 2.8.2).

Example

Query: `http://<sensor IP address>/cmd/set_parameter?operating_mode=measure`

Reply: {

```
"error_code":0,  
"error_text":"success"  
}
```

2.6.3 Scan frequency (scan_frequency, scan_frequency_measured)

The parameter `scan_frequency` defines the set point for the rotational speed of the sensor head and therefore the number of scans recorded per second (see section 3.1 for details). For the R2000 valid values range from 10 Hz to 50 Hz with steps of 1 Hz (default is 35 Hz). Non-integer values are automatically rounded to integer values.

The parameter `scan_frequency_measured` reads the actual value of the rotational speed of the sensor head with a resolution of 0.1 Hz. It is a read-only parameter.

Example

Query: `http://<sensor IP address>/cmd/get_parameter?list=scan_frequency;scan_frequency_measured`

Reply: {

```
"scan_frequency":35,  
"scan_frequency_measured":34.900000,  
"error_code":0,  
"error_text":"success"  
}
```



2.6.4 Scan direction (scan_direction)

The parameter `scan_direction` defines the direction of rotation of the sensors head. User applications can choose between clockwise rotation (`cw`) or counter-clockwise rotation (`ccw`). Please refer to sections 3.1.1 and 3.1.2 on how these settings are related to the sensor coordinate system and the scan data output.

Example

Query: `http://<sensor IP address>/cmd/set_parameter?scan_direction=ccw`

Reply: {

```
"error_code":0,  
"error_text":"success"  
}
```

2.6.5 Scan resolution (samples_per_scan)

The parameter `samples_per_scan` defines the number of samples recorded during one revolution of the sensor head (see section 3.1 for details). Currently, only a number of discrete values are supported. Table 2.1 lists all valid values for the R2000 UHD and HD devices. Requesting any other number of samples per scan results into an error message.

Please note:

The number of `samples_per_scan` multiplied by the `scan_frequency` gives the *sample rate*, i.e. the number of measurements per second. The sensor supports sampling rates between `sampling_rate_min` and `sampling_rate_max` (see section 2.4). Thus the number of `samples_per_scan` indirectly also limits the maximum value for the parameter `scan_frequency` (and vice versa). Therefore table 2.1 denotes the maximum scan frequency as well.

Please note:

The values 1680, 2100 and 2800 for parameter `samples_per_scan` are available for devices with firmware v1.21 or newer, only.

Example

Query: `http://<sensor IP address>/cmd/set_parameter?samples_per_scan=3600`

Reply: {

```
"error_code":0,  
"error_text":"success"  
}
```

samples per scan	angular resolution	max. scan frequency	sampling rate (maximum)
25 200	0.014°	10 Hz	252 kHz
16 800	0.021°	15 Hz	252 kHz
12 600	0.029°	20 Hz	252 kHz
10 080	0.036°	25 Hz	252 kHz
8400	0.043°	30 Hz	252 kHz
7200	0.050°	35 Hz	252 kHz
6300	0.057°	40 Hz	252 kHz
5600	0.064°	45 Hz	252 kHz
5040	0.071°	50 Hz	252 kHz
4200	0.086°	50 Hz	210 kHz
3600	0.100°	50 Hz	180 kHz
2800	0.129°	50 Hz	140 kHz
2400	0.150°	50 Hz	120 kHz
2100	0.171°	50 Hz	105 kHz
1800	0.200°	50 Hz	90 kHz
1680	0.214°	50 Hz	84 kHz
1440	0.250°	50 Hz	72 kHz
1200	0.300°	50 Hz	60 kHz
900	0.400°	50 Hz	45 kHz
800	0.450°	50 Hz	40 kHz
720	0.500°	50 Hz	36 kHz
600	0.600°	50 Hz	30 kHz
480	0.750°	50 Hz	24 kHz
450	0.800°	50 Hz	23 kHz
400	0.900°	50 Hz	20 kHz
360	1.000°	50 Hz	18 kHz
240	1.500°	50 Hz	12 kHz
180	2.000°	50 Hz	9 kHz
144	2.500°	50 Hz	8 kHz
120	3.000°	50 Hz	6 kHz
90	4.000°	50 Hz	5 kHz
72	5.000°	50 Hz	4 kHz

(a) R2000 UHD devices

samples per scan	angular resolution	max. scan frequency	sampling rate (maximum)
8400	0.043°	10 Hz	84 kHz
7200	0.050°	11 Hz	80 kHz
6300	0.057°	13 Hz	82 kHz
5600	0.064°	15 Hz	84 kHz
5040	0.071°	16 Hz	81 kHz
4200	0.086°	20 Hz	84 kHz
3600	0.100°	23 Hz	83 kHz
2800	0.129°	30 Hz	84 kHz
2400	0.150°	35 Hz	84 kHz
2100	0.171°	40 Hz	84 kHz
1800	0.200°	46 Hz	83 kHz
1680	0.214°	50 Hz	84 kHz
1440	0.250°	50 Hz	72 kHz
1200	0.300°	50 Hz	60 kHz
900	0.400°	50 Hz	45 kHz
800	0.450°	50 Hz	40 kHz
720	0.500°	50 Hz	36 kHz
600	0.600°	50 Hz	30 kHz
480	0.750°	50 Hz	24 kHz
450	0.800°	50 Hz	23 kHz
400	0.900°	50 Hz	20 kHz
360	1.000°	50 Hz	18 kHz
240	1.500°	50 Hz	12 kHz
180	2.000°	50 Hz	9 kHz
144	2.500°	50 Hz	8 kHz
120	3.000°	50 Hz	6 kHz
90	4.000°	50 Hz	5 kHz
72	5.000°	50 Hz	4 kHz

(b) R2000 HD devices

Table 2.1: List of valid values for parameter `samples_per_scan`

2.7 HMI / Display configuration

2.7.1 Parameter overview

This section lists all (global) parameters that are available to configure the sensors human machine interface (HMI) consisting of the heads LED display and two push-buttons.

parameter name	type	description	access	default
hmi_display_mode	enum	normal operation display mode	RW	static_logo
hmi_language	enum	display language: english, german	RW	english
hmi_button_lock	bool	lock HMI buttons: on / off	RW	off
hmi_parameter_lock	bool	set HMI to read-only: on / off	RW	off
locator_indication	bool	LED locator indication: on / off	RW	off
<i>display mode parameters (see chapter 4)</i>				
hmi_static_logo	binary	bitmap image for mode static_logo	RW	P+F logo
hmi_static_text_1	string	text line 1 for mode static_text (max. 30 chars)	RW	"Pepperl+Fuchs"
hmi_static_text_2	string	text line 2 for mode static_text (max. 30 chars)	RW	"R2000"
hmi_application_bitmap	binary	bitmap image for mode application_bitmap	vRW	<empty>
hmi_application_text_1	string	text line 1 for application_text (max. 30 chars)	vRW	<empty>
hmi_application_text_2	string	text line 2 for application_text (max. 30 chars)	vRW	<empty>

The display mode parameters allow client application to directly access the HMI LED display. Please refer to chapter 4 for a detailed description on using these capabilities.



2.7.2 HMI display mode (`hmi_display_mode`)

The parameter `hmi_display_mode` controls the content of the HMI LED display during normal operation, i.e. while neither warnings nor errors are displayed and the user did not activate the HMI menu. Depending on the device family, the following display modes are available:

Display mode	Device family	Description
off	all	Display is blank.
static_logo	all	Show a static logo.
static_text	all	Show two lines of static text.
bargraph_distance	OMDxxx-R2000	Show visualization of measured distances.
bargraph_echo	OMDxxx-R2000	Show visualization of measured echo values.
bargraph_reflector	OMDxxx-R2000	Show visualization of high echo targets.
application_bitmap	OMDxxx-R2000	Show an application-provided bitmap.
application_text	OMDxxx-R2000	Show two lines of application-provided text.

The setting of `hmi_display_mode` is stored into non-volatile memory, i.e. it is preserved during a power cycle.

2.7.3 HMI display language (`hmi_language`)

The parameter `hmi_language` controls the language of text messages (menu, warnings, errors) shown by the HMI LED display. Currently the setting `english` and `german` are available. The current setting is stored into non-volatile memory, i.e. it is preserved during a power cycle.

2.7.4 HMI button lock (`hmi_button_lock`)

The boolean parameter `hmi_button_lock` allows to disable the HMI buttons on the sensors front. If set to `on` any push of a button is ignored. This enables client applications to deny users access to the HMI menu of the sensor.

Please note, that locking the buttons also prevents access to read-only information like the current Ethernet configuration. If this is not intended consider using the parameter `hmi_parameter_lock` instead.

2.7.5 HMI parameter lock (`hmi_parameter_lock`)

Protocol version 1.01 adds the boolean parameter `hmi_parameter_lock` which allows to disable parameter changes via the HMI display menu of the sensor. This enables client applications to prevent users from changing sensor parameters while retaining the possibility to determine current settings for parameters available from the HMI menu (e.g. current Ethernet configuration).

2.7.6 Locator indication (`locator_indication`)

The parameter `locator_indication` temporarily activates a distinctive blink pattern for the Power and Q2 LEDs. This function can be used to identify a specific R2000 device if multiple devices are installed. The locator indication function is automatically disabled after reboot, power cycle and factory reset.



2.8 System status

2.8.1 Parameter overview

The following (read only) parameters can be accessed to get status information from the sensor.

parameter name	type	unit	description	access
<i>status information</i>				
status_flags	bitfield	—	sensor status flags (see section 2.8.2)	RO
load_indication	uint	%	current system load (0 %...100 %)	RO
<i>time information</i>				
system_time_raw	ntp64	—	raw system time (see section 3.1.5)	RO
up_time	uint	min	time since power-on	RO
power_cycles	uint	—	number of power cycles	RO
operation_time	uint	min	overall operating time	RO
operation_time_scaled	uint	min	overall operating time scaled by temperature	RO
<i>operating conditions</i>				
temperature_current	int	°C	current operating temperature	RO
temperature_min	int	°C	minimum lifetime operating temperature (power-up update delay 15min)	RO
temperature_max	int	°C	maximum lifetime operating temperature (power-up update delay 15min)	RO
contamination	uint	%	contamination of sensor cover	RO
Note: This parameter currently returns always zero.				

Example

Query: `http://<sensor IP address>/cmd/get_parameter?list=up_time;power_cycles`

Reply: {

```
"up_time":44,  
"power_cycles":22,  
"error_code":0,  
"error_text":"success"  
}
```

2.8.2 System status flags (status_flags)

The read-only parameter `status_flags` (see section 2.8) provides an array of system status flags:

bit	flag name	description
<i>Generic</i>		
0	initialization	System is initializing, valid scan data not available yet
2	scan_output-muted	Scan data output is muted by current system configuration (see section 2.6.2)
3	unstable_rotation	Current scan frequency does not match set value
4	skipped_packets	Preceding scan data packets have been skipped due to connection issues. This might occur if the client does not receive data fast enough.
<i>Warnings</i>		
8	device_warning	Accumulative flag – set if device displays any warning
10	low_temperature_warning	Current device-internal temperature below warning threshold (0 °C)
11	high_temperature_warning	Current device-internal temperature above warning threshold (80 °C)
12	device_overload	Overload warning – sensor CPU overload is imminent
<i>Errors</i>		
16	device_error	Accumulative flag – set if device displays any error
18	low_temperature_error	Current device-internal temperature below error threshold (-10 °C)
19	high_temperature_error	Current device-internal temperature above error threshold (85 °C)
20	device_overload	Overload error – sensor CPU is in overload state
<i>Defects</i>		
30	device_defect	Accumulative flag – set if device detected an unrecoverable defect

System status flags are similar to scan data header status flags (see section 3.4.3) but provide up-to-date information on the current device status (not associated to specific scan data).

Please note:

All flags not listed in the above table are reserved and should be ignored.

2.8.3 System load indication (`load_indication`)

The status variable `load_indication` gives a rough indication of the current CPU load of the sensor:

- **0 % – System is idle**
The system is idle, if the HMI Display is disabled (`hmi_display_mode == 0`) and there is no active scan data output running (neither TCP nor UDP).
- **100 % – System is overloaded**
The system may go into overload if too many clients are requesting scan data via active TCP/UDP connections. In this case nominal operation of the R2000 cannot be guaranteed! Please reduce system load by disabling HMI display, reducing number of TCP/UDP connections or reducing scan resolution.



3 Scan data output using TCP or UDP

3.1 Principles of scan data acquisition

The R2000 is a *laser scanner* designed to periodically measure distances within a full 360° field of view while rotating with a constant frequency defined by the parameter `scan_frequency` (see section 2.6). The measurements are aggregated into *scans*. A single scan corresponds to one revolution of the sensor head, and yields a sequence of *scan points* (also called *samples*). The number of scan points within a scan is defined by the parameter `samples_per_scan` (see section 2.6).

Each scan point is comprised of a distance value for a corresponding angle as well as an echo amplitude. However, since measurements are performed with a uniform angular resolution (depending on the parameter `samples_per_scan`), the actual scan data output typically just gives distance and amplitude data for each sample. The corresponding angular reading can be reconstructed by adding up the angular increments from the starting angle of the scan.

The output format of scan data depends on the scan data packet type used – please refer to section 3.4 for further details. The following subsections describe various basic concepts of the scan data representation used by the R2000.

3.1.1 Sensor coordinate system

The sensor coordinate system is defined as right-handed Cartesian coordinate system. Figure 3.1 shows this coordinate system for the top view and one side view of the sensor: The *origin* is located at the point of intersection of the axis of rotation and the axis of the laser beam. The *X-axis* points to the sensor front – opposite to the connection jacks at the back side of the sensor. The *Y-axis* is located perpendicular to the X-axis and parallel to the base-plate of the sensor (pointing upwards in fig. 3.1a). The *Z-axis* is collinear to the axis of rotation (pointing upwards in fig. 3.1b).

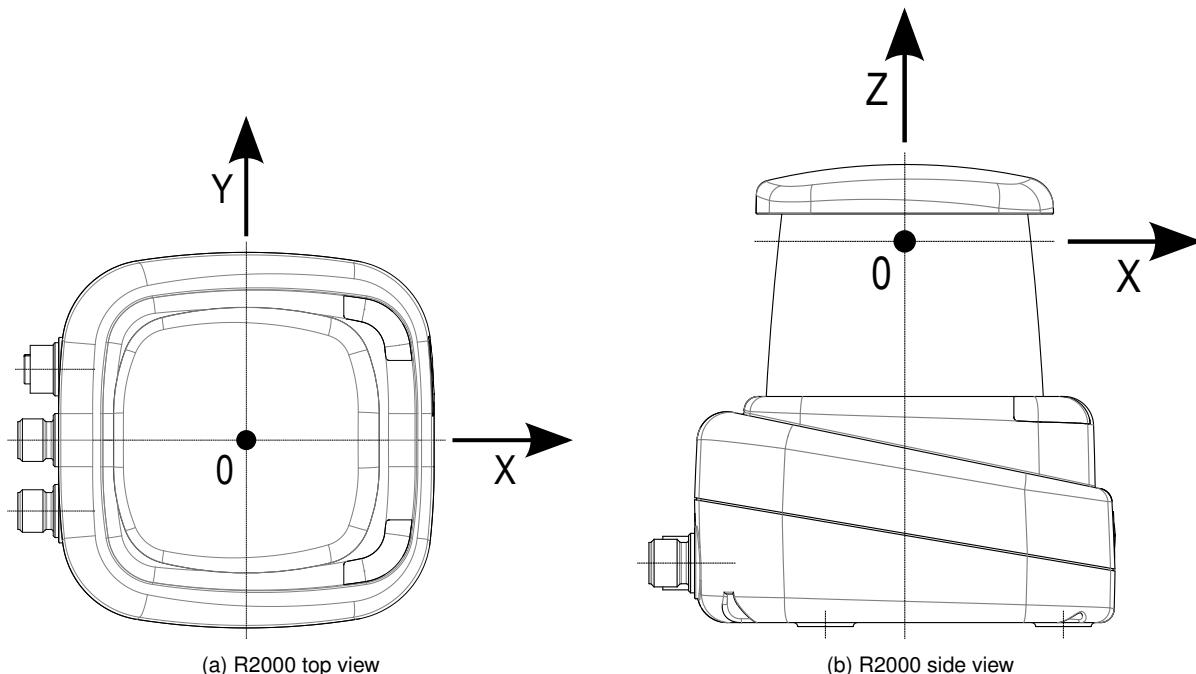


Figure 3.1: Sensor coordinate system



3.1.2 Scan data coordinate system

The plane formed by the X-axis and the Y-axis of the sensor coordinate system is called *scan plane*. All measurements of the laser scanner are recorded within this plane. Scan data acquisition is performed sequentially in the direction of head rotation around the origin of the scan plane. Therefore scan data is typically represented within a polar coordinate system (see fig. 3.2a). The pole of the coordinate system is defined by the axis of rotation (Z-axis of the sensor coordinate system). The reference for angle measurements (polar axis) is equivalent to the X-axis of the sensor coordinate system (pointing upwards in fig. 3.2a).

During nominal operation scan points are continuously recorded using a uniform *angular increment* and direction of rotation. Both, angular increment and direction of rotation, can be configured by global device parameters (see section 2.6). By default the laser scanner rotates in mathematically positive direction. This direction is called *counter-clockwise* (abbreviated *ccw*) – the angular increment between two subsequent scan points has a positive value. The opposite direction is accordingly called *clockwise* (abbreviated *cw*) – the angular increment between two subsequent scan points has a negative value.

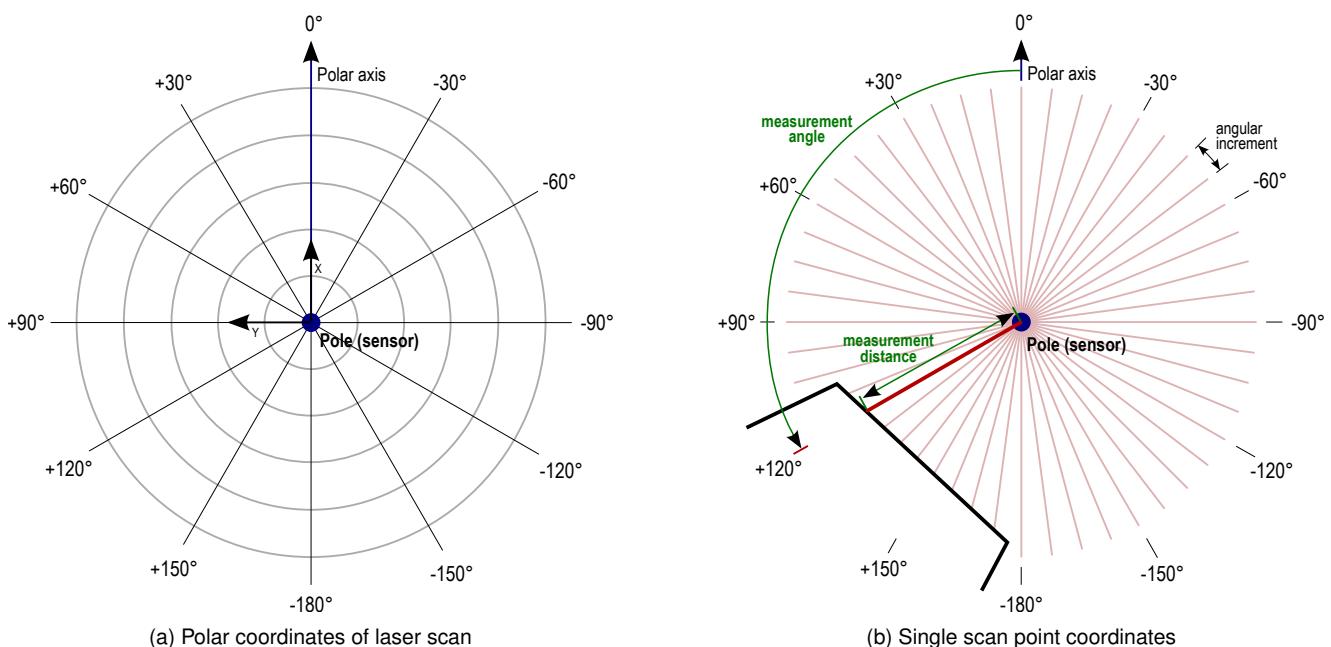


Figure 3.2: Laser scan within sensor scan plane

Figure 3.2b shows an example for a laser scan with an angular increment of 7.5° . The *measurement angle* of a single scan point (angular coordinate) is calculated within the scan plane with reference to the polar axis. The measurement distance (radial coordinate) is determined by the distance from the center of rotation (pole) to the object hit by the laser beam. Angular coordinates within the 360° field of view are specified with a value range of $[-180^\circ; 180^\circ]$ including -180° but excluding 180° .

3.1.3 Distance readings

Distance readings are typically output as integer value as defined by the scan data packet type (see section 3.4). In case of invalid measurements (e.g. no echo detected or distance out of range) the distance reading is set to an error substitution value: the biggest representable integer value for a distance value (e.g. 0xFFFFFFFF for an `uint32` typed distance value).

Please note:

The measurement resolution and measurement range are limited by the physical capabilities of the sensor as listed in the sensor data-sheet. This information is also available by means of the read-only variables `radial_resolution`, `radial_range_min` and `radial_range_max` (see section 2.4).

3.1.4 Echo amplitude readings

For each measurement of the sensor optional amplitude data is available to the client. Amplitude data is output as dimensionless linear values with a fixed resolution of 12 bit.

On principle, amplitude data can deliver an estimate of the *relative* reflectivity of an object only. Measured amplitude depends on the surface properties of the target object (its *absolute* reflectivity), its distance to the sensor, the angle of incidence of the sensors laser beam on the target surface, etc. – therefore a direct comparison of amplitude data is only viable for object surfaces under similar observation conditions.

Please note:

Please note that amplitude data is not calibrated. Thus amplitude data of different sensor devices may not be identical even under similar observation conditions!

The least significant values of the 12 bit amplitude data are reserved for the following special values:

value	name	description
0	no echo	receiver detected no echo
1	blinding	receiver overloaded due to excessive echo amplitude
2	error	unable to measure echo amplitude
3-31	reserved	reserved for internal use
>31	amplitude	measured echo amplitude value

All values in the range of 3 to 31 are reserved for internal use. The smallest real amplitude value (that has been actually measured) is 32.

3.1.5 Timestamps

The R2000 devices provide two types of timestamps:

- **raw timestamps**

Raw timestamps are generated by an internal system clock that starts counting from zero at power-on. Its resolution is better than 1 ms and its drift is below 100 ppm. Raw time is always incrementing without any discontinuities or overflows.

- **synchronised timestamp**

A synchronised timestamp is using a clock source that is synchronized to an external time server. Please note, that these timestamps may be affected by discontinuities due to time server synchronisation.

Timestamps are always provided in 64bit NTP timestamp format (see section 2.1.8 for details). The raw system time can be accessed via the device parameter `system_time_raw` (see section 2.8). When `system_time_raw` is read using `get_parameter` the device will return the raw system time for the point in time, when the command has been received. Please note that both sending the request for a timestamp and receiving the reply with the timestamp are affected by the non-deterministic HTTP transmission delay.

Please note:

This feature is not completely implemented yet! Currently, synchronized timestamps are not available and are output as zero.



3.2 Principles of scan data output

3.2.1 Introduction

In order to receive scan data from the laser scanner the client application needs to establish a *scan data connection* to the sensor. Basically the laser scanner supports two different types of data channels: TCP and UDP. TCP channels provide a secure and error proof channel for transmission of scan data at the cost of potentially unpredictable latency. In contrast, UDP channels allow data transmission with minimum latency at the expense of potential unrecoverable data corruption or data loss. Both TCP and UDP data channels are managed using the HTTP command interface.

For typical applications the following steps are necessary to use scan data output:

1. Set up global configuration of the scanner (see chapter 2), if necessary
2. Establish a data channel to the sensor (see section 3.3.1 and section 3.3.2)
3. Configure scan data output (see section 3.3.6), if necessary
4. Start scan data transmission (see section 3.3.4)
5. Receive scan data from the device (see section 3.4)
6. Stop scan data transmission (see section 3.3.5)
7. Terminate the data channel to the sensor (see section 3.3.3)

Section 3.3 covers the required commands for managing scan data output in detail.

3.2.2 Scan data connection handles

The R2000 supports parallel scan data connections to multiple clients. In order to configure and control these connections individually, each connection is identified by a unique connection *handle*. A handle is defined as random alpha-numeric string of maximal 16 characters. The sensor ensures that each handle is used for only one active scan data connection. Applications should not make any further assumption regarding the structure of a handle as implementation details might change with new firmware versions (see also below).

Compatibility to handle implementation of R2000 firmware v1.0x

Connection handles have been specified as *random* alpha-numeric string since the first version of the Ethernet communication protocol. Unfortunately, R2000 firmware versions prior to v1.20 implemented a rather systematic handle generation algorithm, that caused subsequent handles to receive linear increasing signatures. With firmware v1.20 this implementation has been updated to a more random handle generation pattern.

This implementation alteration should cause no issues with most client applications. However, if a client application relied on the specific handle generation pattern of firmware v1.0x, it needs to be modified to work with the new implementation of firmware v1.20 or later. For backwards compatibility reasons, current firmware versions offer an option to revert the old handle generation pattern. To activate this option, the boolean parameter `deprecated_handle_generation` needs to be set to `on` using the command `set_parameter`. The parameter is stored into non-volatile memory, i.e. it needs to be set only once. Its default value is `off`.

Please note:

The parameter `deprecated_handle_generation` will be removed in future firmware versions. It is strongly recommended to adapt client application to the updated handle generation pattern.



3.2.3 Scan data connection watchdog

By default each scan data connection (identified by a handle) features a watchdog timer. If a data channel is not used within a defined time period the associated scan data output will be stopped, the data channel will be closed and the data channel handle will be invalidated by the sensor. This way the device can free up precious resources for new scan data connections that would be otherwise permanently blocked by "zombie" connections.

In order to prevent a watchdog timeout, the client needs to feed the watchdog on regular basis. This can be done with the command `feed_watchdog` (see section 3.3.8) or using "in-line" watchdog feeds for TCP scan data connections (see section 3.3.9). Each call resets the watchdog timer.

The watchdog timeout period can be configured by the client application individually for each scan data connection using the parameters `watchdog` and `watchdogtimeout` of the commands `request_handle_udp` (see section 3.3.1), `request_handle_tcp` (see section 3.3.2) and `set_scanoutput_config` (see section 3.3.6). The parameter `watchdogtimeout` specifies the timeout period within the range of 1 s up to 500 s. The parameter `watchdog` enables (value `on`) or disables (value `off`) the watchdog. Per default the watchdog is enabled with a timeout period of 60 s.

Please note:

Although the watchdog timeout period (`watchdogtimeout`) can be specified with a resolution of 1 ms, the effective internal resolution used by current firmware versions is about 10 s. Client software should not rely on shorter reaction times.

Please note:

Enabling the watchdog (`watchdog`) or changing the watchdog timeout period (`watchdogtimeout`) using the command `set_scanoutput_config` implicitly feeds the watchdog (i.e. the watchdog timeout is reset).

3.2.4 Scan data output customization

A client may customize some properties of how scan data is output over a scan data channel. These configuration settings are specific to a single data connection identified by the unique connection handle. The settings can be set while initiating a new scan data connection using `request_handle_tcp` (see section 3.3.2) and `request_handle_udp` (see section 3.3.1), or can be changed for an existing scan data connection using `set_scanoutput_config` (see section 3.3.6).

Selecting a start angle

A client may configure the (polar) angle of the first scan point within a scan (index 0) using the parameter `start_angle` (see section 3.3.6). By default it is set to -180.0° (i.e. `start_angle = -1800000`). Subsequent scan points (index $(n + 1)$) within the scan data stream are ordered according to the current sensor head rotation direction. The value of `start_angle` refers to the measurement angle of the scan data coordinate system (see section 3.1.2).

Limiting number of scan points

Protocol version 1.01 adds the parameter `max_num_points_scan` to the list of customizable options for a scan data connection. This parameter allows to limit the number of scan points that are output over a scan data connection. In contrast to the global parameter `samples_per_scan`, which controls how many samples per scan are *recorded* by the sensor, the setting of `max_num_points_scan` affects the number of scan points *output* for a specific scan data connection only. The parameter is specified as unsigned integer (`uint`) and accepts any non-negative number. The value 0 is recognized as special case for 'no limitation', i.e. the sensor outputs always all points of scan. This is also the default value.

If `max_num_points_scan` is set to a value below `samples_per_scan`, the client application receives less scan points than the sensor records. In combination with the parameter `start_angle` this allows client application to obtain only a segment (sector) of a scan instead of all recorded scan points. Figure 3.3 visualizes such a setup. This can be very useful to reduce data traffic if the full 360° field of view of the sensor is not needed.

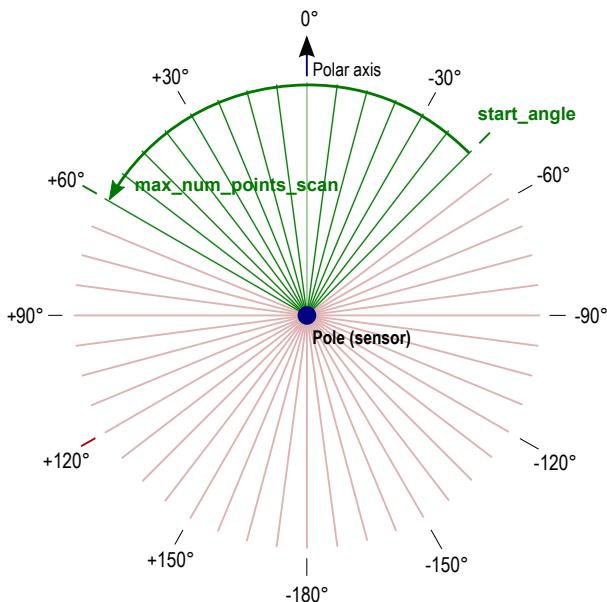


Figure 3.3: Limitation of scan output to a segment

3.2.5 Using multiple concurrent scan data connections

As pointed out before, the scan data protocol is designed to support multiple concurrent scan data connections. However, CPU resources are limited for current R2000 devices. It depends on the measuring configuration of the sensor (see section 2.6) how many concurrent connections can be operated without adverse effects due to system overload.

It is the responsibility of the client application software to ensure that the system load resulting from concurrent data channels can be handled by the sensor (see section 1.1). Neither a successful request of a connection handle (see sections 3.3.1 and 3.3.2) nor a successful connection establishment guarantee that the requested amount of data can be continuously provided by the sensor in real time. System load of the device can be monitored by reading the system status variable `load_indication` – see section 2.8.

The maximum number of connections is limited to the value of `max_connections` (see section 2.4).

Please note:

A single client data channel can be handled by the sensor without any restrictions.

3.3 Commands for managing scan data output

The subsequent sections describe all commands.

3.3.1 request_handle_udp – request for an UDP-based scan data channel

The command `request_handle_udp` is used to request a handle for an UDP-based scan data transmission from the sensor to the client. If successful the sensor will send scan data to the client using the target IP address and UDP port specified at the handle request. Figure 3.4 gives an overview on the communication between sensor and client when using an UDP-based channel for scan data output.

Command arguments

The command `request_handle_udp` accepts the following arguments:

argument name	type	unit	description	default
address	ipv4	–	required: target IP address of the client	–
port	uint	–	required: target port for UDP data channel (client side)	–
watchdog	bool	on / off	optional: enable or disable connection watchdog	on
watchdogtimeout	uint	1 ms	optional: connection watchdog timeout period	60 000 ms
packet_type	enum	–	optional: scan data packet type (see section 3.4)	A
start_angle	int	1/10 000°	optional: angle of first scan point for scan data output	-1800000
max_num_points_scan	uint	samples	optional: limit number of points in scan data output	0 (unlimited)

Please note that `request_handle_udp` optionally accepts all arguments of the `set_scanoutput_config` command (see section 3.3.6) – except the argument `handle`. This way the initial configuration of the scan data output can be already specified during data channel initiation.

Command return values

- `handle` – unique (random) alpha-numeric string as identifier (handle) for the new UDP data channel

During a valid command call the scanner creates a new UDP channel to the client using the specified target IP address and port number. The scanner may refuse a request to create a new UDP channel, e.g. if the maximum number of concurrent client connections is exceeded. In case of an error the returned value for `handle` is invalid and `error_code` / `error_text` return details regarding the cause of the negative response (see section 1.2.6).

Please note:

Since an UDP scan data connection is established from the sensor to the client ("incoming connection") it is prone to be blocked by firewall software. Please ensure that your firewall settings allow incoming UDP connections from the sensor IP address to your client application.

Please note:

Applications should not make any assumption regarding the structure of a handle. Handles should be treated as random alpha-numeric string of max. 16 characters.

Command example

Query: `http://<sensor IP address>/cmd/request_handle_udp?address=192.168.10.20&port=54321&packet_type=C`

Reply: {

```
"handle": "s10",
"error_code": 0,
"error_text": "success"
}
```

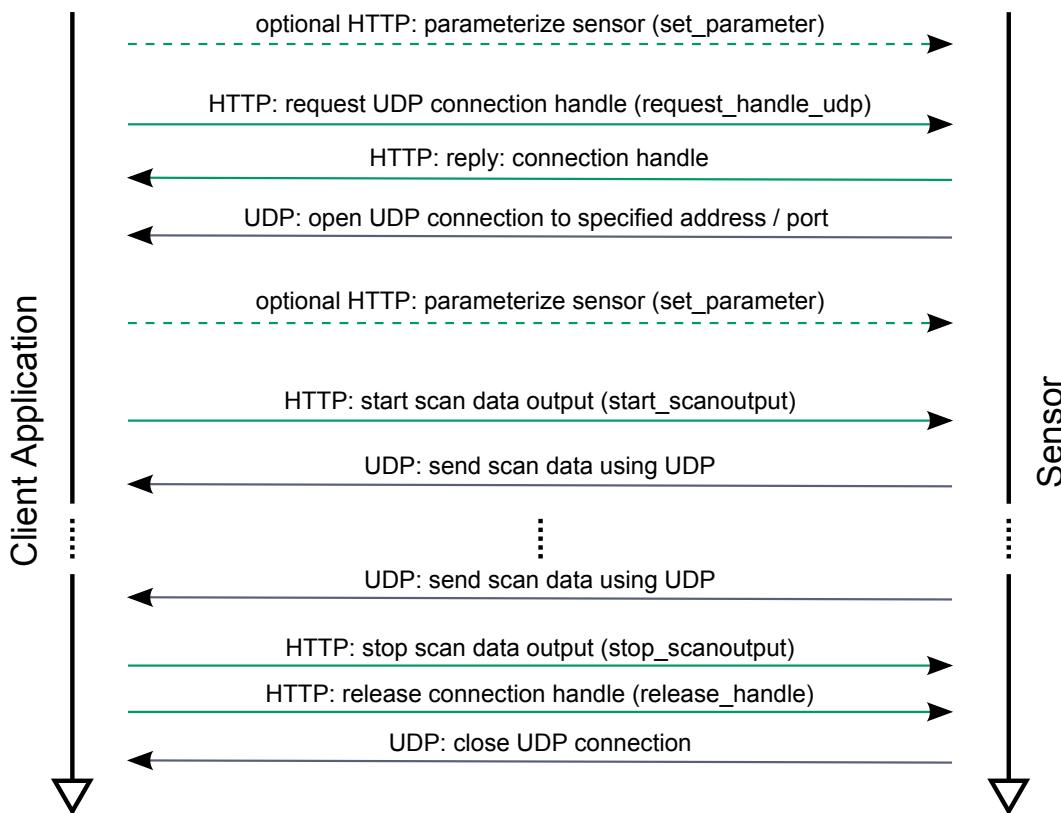


Figure 3.4: Timeline: scan data transmission using UDP

3.3.2 `request_handle_tcp` – request for a TCP-based scan data channel

The command `request_handle_tcp` is used to request a handle for a TCP-based scan data transmission from the sensor to the client. If successful, the client is allowed to create a new TCP connection to the sensor in order to receive scan data. Figure 3.5 gives an overview on the communication between sensor and client when using an TCP-based channel for scan data output.

Command arguments

The command `request_handle_tcp` accepts the following arguments:

argument name	type	unit	description	default
address	ipv4	–	optional: IP address of the client	(see below)
port	uint	–	optional: desired port for client connection (sensor side)	(see below)
watchdog	bool	on / off	optional: enable or disable connection watchdog	on
watchdogtimeout	uint	1 ms	optional: connection watchdog timeout period	60 000 ms
packet_type	enum	–	optional: scan data packet type (see section 3.4)	A
start_angle	int	1/10 000°	optional: angle of first scan point for scan data output	-1800000
max_num_points_scan	uint	samples	optional: limit number of points in scan data output	0 (unlimited)

Please note that `request_handle_tcp` optionally accepts all arguments of the `set_scanoutput_config` command (see section 3.3.6) – except the argument `handle`. This way the initial configuration of the scan data output can be already specified during data channel initiation.

Command return values

- `handle` – unique (random) alpha-numeric string as identifier (`handle`) for the new TCP data channel
- `port` – port number for the new TCP data channel

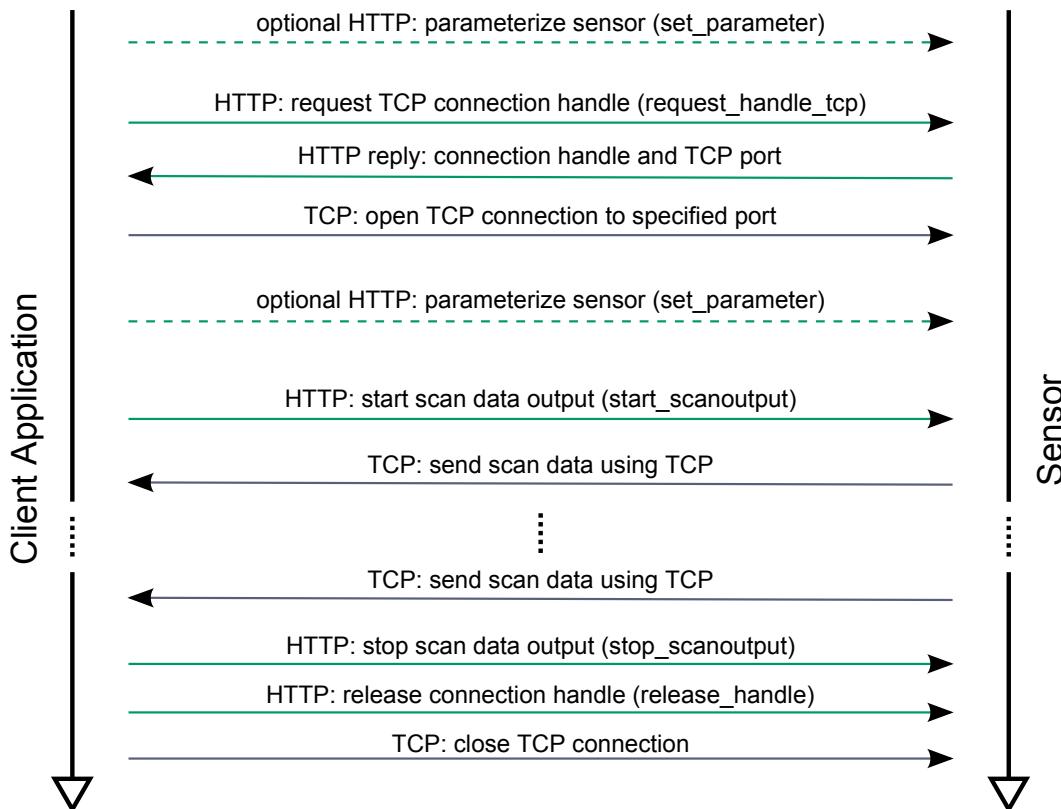


Figure 3.5: Timeline: scan data transmission using TCP

On success the sensor returns a TCP port number in `port`, which is now open for a client data connection. Note, that each port accepts a single TCP connection only! If the argument `address` had been specified upon calling `request_handle_tcp`, the scanner accepts an IP connection originating from the given IP address only (using the returned `handle`).

Using the argument `port` the client can try to reserve a specific port for its TCP connection. If this port is already in use, `request_handle_tcp` returns an error. If the argument `port` is not specified the sensor autonomously selects an ephemeral port within the range 32768 – 61000.

A call to `request_handle_tcp` might fail, e.g. if the maximum number of concurrent client connections is reached. In case of an error the returned values for `handle` and `port` are invalid and `error_code` / `error_text` provide error details (see section 1.2.6).

Please note:

It is not recommended to request a TCP connection to a fixed port number using the command argument `port`. A fixed port might be blocked by other applications or a previous connection. It is recommended to use automatic port selection by the sensor instead.

Please note:

Applications should not make any assumption regarding the structure of a handle. Handles should be treated as random alpha-numeric string of max. 16 characters.

Command example

Query: `http://<sensor IP address>/cmd/request_handle_tcp?packet_type=A&watchdogtimeout=1000&start_angle=0`

Reply: {

```

    "port":39731,
    "handle":"s22",
    "error_code":0,
    "error_text":"success"
  }

```



3.3.3 release_handle – release a data channel handle

Using the command `release_handle` the client can release a data channel handle. Any active scan data output using this handle will be stopped immediately. An associated UDP-based data channel is closed by the sensor itself. An associated TCP-based data channel should be closed by the client.

Command arguments

argument name	type	description
handle	string	handle for scan data channel (max.16 chars) (required argument – always specified first)

Command example

Query: `http://<sensor IP address>/cmd/release_handle?handle=s22`

Reply: {
 "error_code":0,
 "error_text":"success"
}

3.3.4 start_scanoutput – initiate output of scan data

The command `start_scanoutput` starts the transmission of scan data for the data channel specified by the given handle. When started, the sensor will begin sending scan data to the client using an established UDP or TCP channel with the given handle – see section 3.3.1 and section 3.3.2. (Re-)starting a scan data transmission also resets the counters for scan number and scan packet number in the scan data header (see section 3.4.2). Scan data output always starts at the beginning of a new scan (with scan number 0 and scan packet number 1).

Command arguments

argument name	type	description
handle	string	handle for scan data channel (max.16 chars) (required argument – always specified first)

Command example

Query: `http://<sensor IP address>/cmd/start_scanoutput?handle=s22`

Reply: {
 "error_code":0,
 "error_text":"success"
}

3.3.5 stop_scanoutput – terminate output of scan data

The command `stop_scanoutput` stops the transmission of scan data for the data channel specified by the given handle. The scan data output stops immediately after the current scan data packet – not necessarily at the end of a full scan.

Please note:

TCP clients might still receive several scan data packets after sending `stop_scanoutput`, due to the TCP stack data queue.

Command arguments

argument name	type	description
handle	string	handle for scan data channel (max.16 chars) (required argument – always specified first)

Command example

Query: `http://<sensor IP address>/cmd/stop_scanoutput?handle=s22`

```
Reply: {
    "error_code":0,
    "error_text":"success"
}
```

3.3.6 set_scanoutput_config – reconfigure scan data output

Using the command `set_scanoutput_config` the client can parametrize scan data output separately for each active scan data output channel. All command arguments solely apply to the *output* of scan data. Customization of (global) parameters referring to the recording of measurements (scan data) is done by use of the command `set_parameter` (see section 2.6).

Command arguments

argument name	type	unit	description	default
handle	string	–	handle for scan data channel (max.16 chars) (required argument – always specified first)	–
watchdog	bool	on / off	optional: enable or disable connection watchdog	on
watchdogtimeout	uint	1 ms	optional: connection watchdog timeout period	60 000 ms
packet_type	enum	–	optional: scan data packet type: A, B, C, (see section 3.4)	A
start_angle	int	1/10 000°	optional: angle of first scan point for scan data output	-1800000
max_num_points_scan	uint	samples	optional: limit number of points in scan data output	0 (unlimited)

It is recommended (but not required) to stop sensor data output while using `set_scanoutput_config`. In case scan data output is active, the point in time when modified configuration settings are applied to the running data stream is non-deterministic. After the new settings are applied, scan data output is suspended until the start of a new scan (skipping scan data packets in-between). If the client application depends on a deterministic switching behavior, it should stop scan data transmission first using `stop_scanoutput`, change settings using `set_scanoutput_config` and finally restart the data stream with `start_scanoutput`.

Parameter start_angle

The user can control the angle for the first scan point of a scan by means of the parameter `start_angle`. The range of valid values is [-1800000; +1800000] including -1800000 (-180°) but excluding +1800000 (180°). The specified value does not have to match the configured angular resolution for scan data acquisition (see section 2.6) – the sensor will start scan data output with the first scan point whose recording angle is equal to or following behind the specified angle in direction of rotation.

Please note:

The command `get_scanoutput_config` (see section 3.3.7) will return the exact user specified value, while the entry “absolute angle of first scan point” within the scan data packet header (see section 3.4.2) will specify the exact value of the first scan point actually used.

Command example

Query: `http://<sensor IP address>/cmd/set_scanoutput_config?handle=s22&packet_type=B&start_angle=-900000`

```
Reply: {
    "error_code":0,
    "error_text":"success"
}
```

3.3.7 get_scanoutput_config – read scan data output configuration

The command `get_scanoutput_config` returns the current scan data output configuration for a specified scan data output channel (UDP or TCP).

Command arguments

argument name	type	description
handle	string	handle for scan data channel (max.16 chars) (required argument – always specified first)
list	string	semicolon separated list of parameter names (optional)

If the argument `list` is not specified the command will return the current value of all available configuration parameters (see section 3.3.6).

Command example

Query: `http://<sensor IP address>/cmd/get_scanoutput_config?handle=s22`

```
Reply: {
    "address":"0.0.0.0",
    "port":39050,
    "watchdog":"on",
    "watchdogtimeout":60000,
    "packet_type":"A",
    "start_angle":-1800000,
    "error_code":0,
    "error_text":"success"
}
```

3.3.8 feed_watchdog – feed connection watchdog

The command `feed_watchdog` feeds the connection watchdog, i.e. each call of this command resets the watchdog timer. Please refer to section 3.2.3 for a detailed description of the connection watchdog mechanism.

Command arguments

argument name	type	description
handle	string	handle for scan data channel (max.16 chars) (required argument – always specified first)

Command example

Query: `http://<sensor IP address>/cmd/feed_watchdog?handle=s36924971`

Reply: {
 "error_code":0,
 "error_text":"success"
}

Please note:

Enabling the watchdog (watchdog) or changing the watchdog timeout period (watchdogtimeout) using the command `set_scanoutput_config` (see section 3.3.6) implicitly feeds the watchdog as well.

3.3.9 TCP in-line watchdog feeds

PFSDP version 1.01 adds support for TCP "in-line" watchdog feeds using the backward channel of an existing bi-directional TCP scan data connection (see section 3.3.2). It allows to feed the connection watchdog, without imposing an HTTP connection for every feed action as required by the existing `feed_watchdog` command (see section 3.3.8).

Feed sequence

In order to feed the watchdog of an existing TCP scan data connection the following byte sequence needs to be send from the client application to the sensor:

0x66 0x65 0x65 0x64 0x77 0x64 0x67 0x04

This 8-byte sequence represents the ASCII string `feedwdg<eot>`, which is recognized by the sensor. The sensor does not send any confirmation whether the watchdog request has been processed. However, since the TCP connection ensures an error free transmission this confirmation is not needed anyway.

Please note:

Due to limitations of the sensor firmware client applications should not send in-line watchdog feed requests more often than once per second (maximum feed frequency of 1 Hz).

Please note:

Enabling the watchdog (watchdog) or changing the watchdog timeout period (watchdogtimeout) using the command `set_scanoutput_config` (see section 3.3.6) implicitly feeds the watchdog as well.



3.4 Transmission of scan data

Scan data is always transmitted within packets. A complete scan is usually transmitted using multiple scan data packets (see section 1.1 for basic design considerations). Each packet comprises of a generic header, a scan data specific header and the actual scan data.

Multiple packet types can be defined to output different sets of scan data information efficiently. These packet types usually follow a standard structure – differing in the bulk scan data only. Within bulk scan data usually each scan point is represented by a structure containing the favored amount of data (distance, amplitude, etc.).

The following sections describe scan data packets in detail.

3.4.1 Basic packet structure

Each data packet has the following basic structure:

type	name	description
uint16	magic	magic byte (0xa25c) marking the beginning of a packet
uint16	packet_type	type of scan data packet
uint32	packet_size	overall size of this packet in bytes (header and payload)
uint16	header_size	size of header in bytes (i.e. offset to payload data)
...	...	packet type specific additional header information
uint8[]	header_padding	0-3 bytes padding (to align the header size to a 32bit boundary)
...	payload_data	packet type specific payload data

Although the structure of the packet usually appears to be fixed, it is highly recommended that client applications always evaluate the entries for packet size and header size since they may change due to future extensions.

The magic byte at the beginning of the packet header is designed to be used as synchronization mark within a continuous data stream. It can be ignored if synchronization is not needed.

The starting address of payload data is always aligned to a 32bit address boundary by using padding bytes within the header (`header_padding`).



3.4.2 Typical structure of a scan data header

A scan data packet contains a scan data header with information on the scan and the scan data itself. The scan data header is designed in ways that each scan data packet can be processed independent of other scan data packets belonging to the same scan.

A typical scan data header has the following structure:

type	name	description
uint16	magic	magic byte (0xa25c) marking the beginning of a packet
uint16	packet_type	type of scan data packet
uint32	packet_size	overall size of this packet in bytes (header and payload)
uint16	header_size	size of header in bytes (i.e. offset to payload data)
uint16	scan_number	sequence number for scan (incremented for every scan, starting with 0, overflows)
uint16	packet_number	sequence number for packet (counting packets of a particular scan, starting with 1)
ntp64	timestamp_raw	raw timestamp of first scan point in this packet (see section 3.1.5)
ntp64	timestamp_sync	synchronized timestamp of first scan point in this packet (see section 3.1.5) Note: Synchronized timestamps are currently not available and are output as zero.
uint32	status_flags	scan status flags (see section 3.4.3)
uint32	scan_frequency	frequency of head rotation (1/1000 Hz)
uint16	num_points_scan	number of scan points (samples) within complete scan (depending on configured FOV)
uint16	num_points_packet	number of scan points within this packet
uint16	first_index	index of first scan point within this packet
int32	first_angle	absolute angle of first scan point in this packet (1/10 000°)
int32	angular_increment	delta angle between two scan points (1/10 000°) (CCW rotation: positive increment, CW rotation: negative increment)
uint32	iq_input	reserved – all bits zero for devices without switching I/Q
uint32	iq_overload	reserved – all bits zero for devices without switching I/Q
uint8[]	header_padding	0-3 bytes padding (to align the header size to a 32bit boundary)
...	scandata	packet type specific scan data

Please note:

The field `num_points_scan` states the total number of scan points *output* for each recorded scan. It is always equal to either `samples_per_scan` or `max_num_points_scan`, whichever is smaller for the specific scan data connection. Please refer to section 3.2.4 for more details on this matter.

Please note:

Angular values specified with a resolution of 1/10 000° are usually prone to rounding errors due to the decimal range of values. They are part of the header for convenience only. Subsequent calculations requiring precise angular values should calculate an exact angle for each scan point by reference to its index number, the configured angular increment and the configured start angle of the scan:

$$\text{CCW rotation: } \text{exact_angle}_{\text{scanpoint}} = \text{start_angle}_{\text{scan}} + \text{index}_{\text{scanpoint}} * \frac{360^\circ}{\text{num_points_scan}}$$

$$\text{CW rotation: } \text{exact_angle}_{\text{scanpoint}} = \text{start_angle}_{\text{scan}} - \text{index}_{\text{scanpoint}} * \frac{360^\circ}{\text{num_points_scan}}$$

3.4.3 Scan data header status flags

Scan data header status flags are similar to system status flags (see section 2.8.2) but provide status information specific to the scan data of a scan data packet. Each scan data header contains an `uint32` entry `status_flags` (see section 3.4.2) comprised of the following flags:

bit	flag name	description
<i>Generic</i>		
0	<code>scan_data_info</code>	Accumulative flag – set if any of the following generic flags is set
1	<code>new_settings</code>	System settings for scan data acquisition changed during recording of this packet. This flag is currently only triggered by write accesses to the global parameter <code>samples_per_scan</code> which can be done by any client (see section 2.2.3). Changes to connection-specific parameters do not trigger this flag (see section 3.3.6)!
2	<code>invalid_data</code>	Consistency of scan data is not guaranteed for this packet.
3	<code>unstable_rotation</code>	Scan frequency did not match set value while recording this scan data packet.
4	<code>skipped_packets</code>	Preceding scan data packets have been skipped due to connection issues. This might occur if the client does not receive data fast enough.
<i>Warnings</i>		
8	<code>device_warning</code>	Accumulative flag – set if device displays any warning
10	<code>low_temperature_warning</code>	Current device-internal temperature below warning threshold (0 °C)
11	<code>high_temperature_warning</code>	Current device-internal temperature above warning threshold (80 °C)
12	<code>device_overload</code>	Overload warning – sensor CPU overload is imminent
<i>Errors</i>		
16	<code>device_error</code>	Accumulative flag – set if device displays any error
18	<code>low_temperature_error</code>	Current device-internal temperature below error threshold (-10 °C)
19	<code>high_temperature_error</code>	Current device-internal temperature above error threshold (85 °C)
20	<code>device_overload</code>	Overload error – sensor CPU is in overload state
<i>Defects</i>		
30	<code>device_defect</code>	Accumulative flag – set if device detected an unrecoverable defect

Please note:

All flags not listed in the above table are reserved and should be ignored.



3.4.4 Scan data packet type A – distance only

Scan data packets of type A have the following structure:

type	name	description
<i>packet header</i>		
uint16	magic	magic byte (0xa25c) marking the beginning of a packet
uint16	packet_type	type of scan data packet: 0x0041 (ASCII character 'A')
uint32	packet_size	overall size of this packet in bytes (header and payload)
uint16	header_size	size of header in bytes (i.e. offset to payload data)
uint16	scan_number	sequence number for scan (incremented for every scan, starting with 0, overflows)
uint16	packet_number	sequence number for packet (counting packets of a particular scan, starting with 1)
ntp64	timestamp_raw	raw timestamp of first scan point in this packet (see section 3.1.5)
ntp64	timestamp_sync	synchronized timestamp of first scan point in this packet (see section 3.1.5) Note: Synchronized timestamps are currently not available and are output as zero.
uint32	status_flags	scan status flags (see section 3.4.3)
uint32	scan_frequency	frequency of head rotation (1/1000 Hz)
uint16	num_points_scan	number of scan points (samples) within complete scan (depending on configured FOV)
uint16	num_points_packet	number of scan points within this packet
uint16	first_index	index of first scan point within this packet
int32	first_angle	absolute angle of first scan point in this packet (1/10 000°)
int32	angular_increment	delta angle between two scan points (1/10 000°) (CCW rotation: positive increment, CW rotation: negative increment)
uint32	iq_input	reserved – all bits zero for devices without switching I/Q
uint32	iq_overload	reserved – all bits zero for devices without switching I/Q
uint8[]	header_padding	0-3 bytes padding (to align the header size to a 32bit boundary)
<i>scan point data</i>		
uint32	distance	measured distance (in mm) Invalid measurements return 0xFFFFFFFF.

Please note:

The field `num_points_scan` states the total number of scan points *output* for each recorded scan. It is always equal to either `samples_per_scan` or `max_num_points_scan`, whichever is smaller for the specific scan data connection. Please refer to section 3.2.4 for more details on this matter.

3.4.5 Scan data packet type B – distance and amplitude

Scan data packets of type B have the following structure:

type	name	description
<i>packet header</i>		
uint16	magic	magic byte (0xa25c) marking the beginning of a packet
uint16	packet_type	type of scan data packet: 0x0042 (ASCII character 'B')
uint32	packet_size	overall size of this packet in bytes (header and payload)
uint16	header_size	size of header in bytes (i.e. offset to payload data)
uint16	scan_number	sequence number for scan (incremented for every scan, starting with 0, overflows)
uint16	packet_number	sequence number for packet (counting packets of a particular scan, starting with 1)
ntp64	timestamp_raw	raw timestamp of first scan point in this packet (see section 3.1.5)
ntp64	timestamp_sync	synchronized timestamp of first scan point in this packet (see section 3.1.5) Note: Synchronized timestamps are currently not available and are output as zero.
uint32	status_flags	scan status flags (see section 3.4.3)
uint32	scan_frequency	frequency of head rotation (1/1000 Hz)
uint16	num_points_scan	number of scan points (samples) within complete scan (depending on configured FOV)
uint16	num_points_packet	number of scan points within this packet
uint16	first_index	index of first scan point within this packet
int32	first_angle	absolute angle of first scan point in this packet (1/10 000°)
int32	angular_increment	delta angle between two scan points (1/10 000°) (CCW rotation: positive increment, CW rotation: negative increment)
uint32	iq_input	reserved – all bits zero for devices without switching I/Q
uint32	iq_overload	reserved – all bits zero for devices without switching I/Q
uint8[]	header_padding	0-3 bytes padding (to align the header size to a 32bit boundary)
<i>scan point data</i>		
uint32	distance	measured distance (in mm) Invalid measurements return 0xFFFFFFFF.
uint16	amplitude	measured amplitude (padded 12bit value – most significant bits are zero) Please see section 3.1.4 for a description of amplitude data values.

Please note:

The field `num_points_scan` states the total number of scan points *output* for each recorded scan. It is always equal to either `samples_per_scan` or `max_num_points_scan`, whichever is smaller for the specific scan data connection. Please refer to section 3.2.4 for more details on this matter.



3.4.6 Scan data packet type C – distance and amplitude (compact)

Scan data packets of type C have the following structure:

type	name	description
<i>packet header</i>		
uint16	magic	magic byte (0xa25c) marking the beginning of a packet
uint16	packet_type	type of scan data packet: 0x0043 (ASCII character 'C')
uint32	packet_size	overall size of this packet in bytes (header and payload)
uint16	header_size	size of header in bytes (i.e. offset to payload data)
uint16	scan_number	sequence number for scan (incremented for every scan, starting with 0, overflows)
uint16	packet_number	sequence number for packet (counting packets of a particular scan, starting with 1)
ntp64	timestamp_raw	raw timestamp of first scan point in this packet (see section 3.1.5)
ntp64	timestamp_sync	synchronized timestamp of first scan point in this packet (see section 3.1.5) Note: Synchronized timestamps are currently not available and are output as zero.
uint32	status_flags	scan status flags (see section 3.4.3)
uint32	scan_frequency	frequency of head rotation (1/1000 Hz)
uint16	num_points_scan	number of scan points (samples) within complete scan (depending on configured FOV)
uint16	num_points_packet	number of scan points within this packet
uint16	first_index	index of first scan point within this packet
int32	first_angle	absolute angle of first scan point in this packet (1/10 000°)
int32	angular_increment	delta angle between two scan points (1/10 000°) (CCW rotation: positive increment, CW rotation: negative increment)
uint32	iq_input	reserved – all bits zero for devices without switching I/Q
uint32	iq_overload	reserved – all bits zero for devices without switching I/Q
uint8[]	header_padding	0-3 bytes padding (to align the header size to a 32bit boundary)
<i>scan point data</i>		
uint20	distance	measured distance (in mm) – maximum representable value is 1 km Invalid measurements return 0xFFFFF.
uint12	amplitude	measured amplitude Please see section 3.1.4 for a description of amplitude data values.

Scan data packets of type C differ from type B in the binary size of the values `distance` and `amplitude` only. For type C these values are encoded as bit fields within a `uint32` type.

Please note:

The field `num_points_scan` states the total number of scan points *output* for each recorded scan. It is always equal to either `samples_per_scan` or `max_num_points_scan`, whichever is smaller for the specific scan data connection. Please refer to section 3.2.4 for more details on this matter.



3.5 Data transmission using TCP

When using a TCP-based channel for scan data transmission scan data will be divided into one or more scan data packets. A new scan will always start with a new scan data packet.

Please note:

Currently scan data is divided into several scan data packets according to the size of an Ethernet frame (typically 1500 bytes).

Please note:

A new scan will be transmitted only after the last scan has been successfully received by the client. If reception of the scan data is delayed due to transmission errors or slow client response, the sensor might skip transmission of single scan packets or complete scans.

3.6 Data transmission using UDP

When using a UDP-based channel for scan data transmission scan data will be divided into several scan data packets according to the size of an Ethernet frame (typically 1500 bytes). A new scan will always start with a new scan data packet.

In case some scan data packets are lost during transmission, no error recovery is provided. The client application can make use of successfully received scan data packets (containing partial scan data), since every scan data packet incorporates a full scan data header and can be processed separately.

Please note:

The sensor uses a special real time (RT) task for UDP scan data output in order to minimize latency. This RT task is currently available for a single UDP client connection only. Additional (parallel) UDP client connections are handled by non-RT tasks and might show inferior time behavior.

4 Working with the HMI LED display

This chapter features a detailed description of the HMI LED display of the R2000 and instructions on using it for displaying application-specific information.

4.1 Technical overview

The R2000 device family features a multi-function HMI LED display. The display is created by an array of 24 LEDs that are mounted on one edge of the rotating sensor head, making use of the so-called *Persistence of Vision (POV)* characteristic of the human eye. By rapid updates of the LED array during the rotation of the sensor head a virtual raster graphic with 24 rows and 252 columns is created. For best readability scan frequencies above 35 Hz are recommended (see parameter `scan_frequency` in section 2.6).

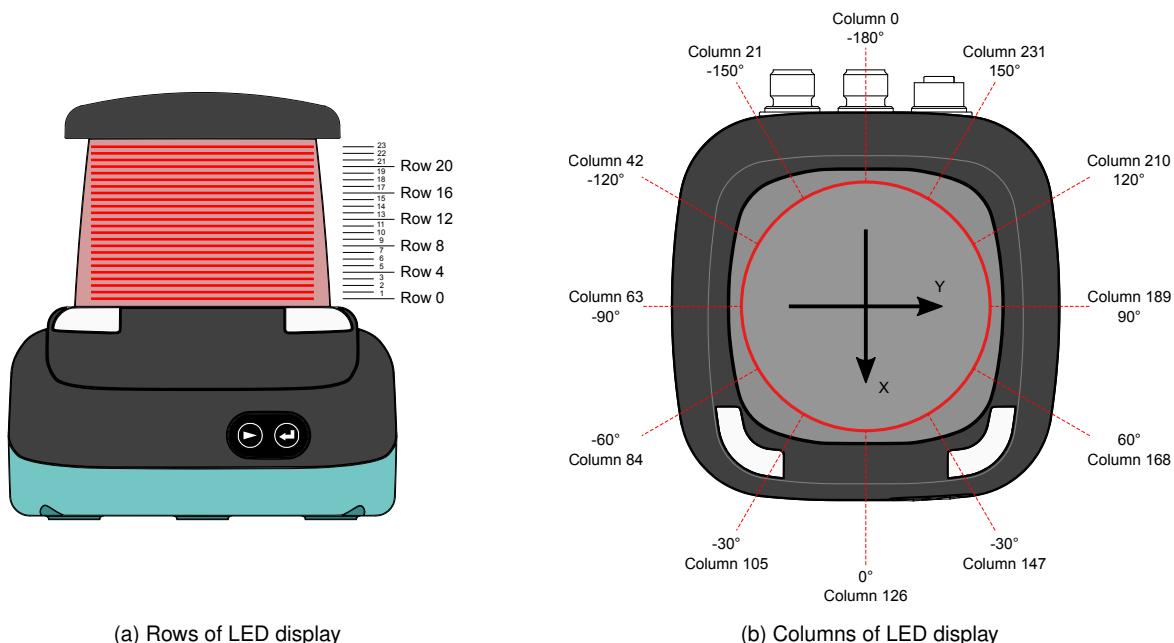


Figure 4.1: HMI display coordinate system

Figure 4.1 shows the positioning of the LED display with respect to the sensor coordinate system (as defined in section 3.1.1). Information on the LED display is usually shown centered at 0° on the front of the sensor (column 126). The display area starts at column 0 on the back of the sensor at -180° . The columns are arranged in mathematical positive order up to column 251 at approximately 178.6° . The transition from column 251 to column 0 on the sensors back is seamless, enabling a usable field of view of full 360° . When rendering the display content the sensor firmware takes the sensors direction of rotation into account. The client application does not need to consider the current value of parameter `scan_direction` (section 2.6) when preparing content for the HMI LED display.

Figure 4.2 shows a two-dimensional representation of the display pixel layout (2D bitmap). This is a simplified view since the curvature and 360° wrap-around nature of the real display are not shown. The physical display area covers approximately 48 mm in height and 170 mm in width. This results into a horizontal pixel density (resolution) of about 38 dpi and a vertical pixel density of about 12 dpi. The three times higher horizontal resolution implies that three horizontal pixels need to be combined in order to show a single square 'pixel' on the HMI LED display.

Application developers can utilize the LED display for showing custom text messages or custom bitmap images. The following sections describe these use-cases in detail.

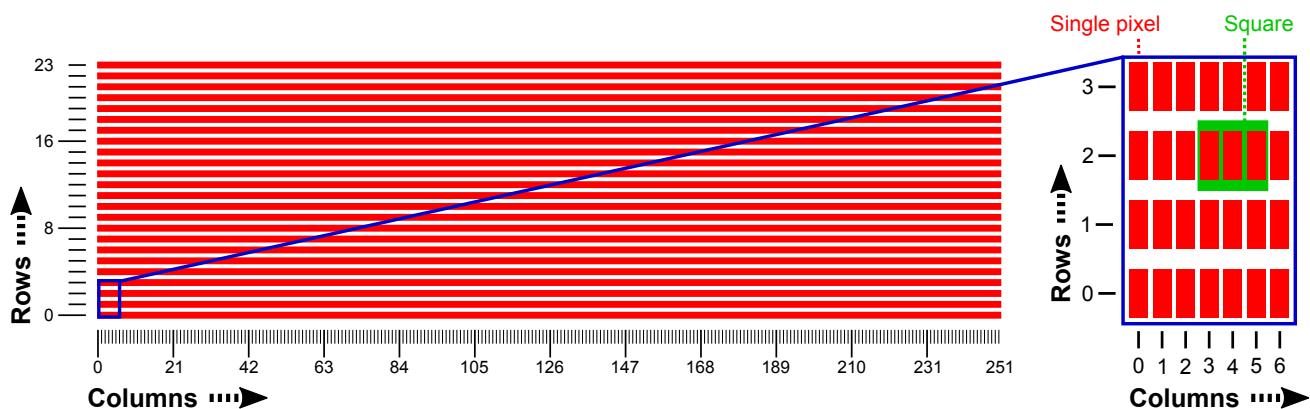


Figure 4.2: HMI display pixel layout (252 x 24 pixels)

4.2 Displaying custom text messages

Using short text messages is the easiest way of showing custom information on the R2000 HMI LED display. The sensor supports two different modes for displaying text: A mode for static text messages that are preserved even after a power-cycle and a mode for rather volatile text messages that are updated by the client application more frequently.

4.2.1 Overview

The text display features two independent lines of text – one in the upper half of the display and one in the lower half. Text is displayed with a fixed width font of 8 pixel height (using 8 of 24 display rows). Each text line is limited to a length of max. 30 characters and shown horizontally centered at the front of the sensor. The display supports a selection of typical special characters (e.g. umlauts) out of the UTF-8 code range. Unsupported special characters are replaced by a question mark character ('?').

4.2.2 Static text messages (static text)

The display mode `static_text` allows client applications to display up to two lines of static text on the HMI LED display. The application text lines are stored in the parameters `hmi_static_text_1` and `hmi_static_text_2` within non-volatile memory, i.e. the content is not lost during a power-cycle. The display mode is especially suited for displaying rarely updated information, e.g. an identification string for the sensor. The parameters `hmi_static_text_1` and `hmi_static_text_2` are reset on request only (e.g. when loading the factory defaults). The default content reads 'Pepperl+Fuchs' and 'R2000'.

Steps for displaying static text messages are:

1. Write text for the upper display line to `hmi_static_text_1` using `set_parameter`.
2. Write text for the lower display line to `hmi_static_text_2` using `set_parameter`.
3. Enable the static text display by setting parameter `hmi_display_mode` to `static_text` using `set_parameter`.

Please note:

Since each write access to `hmi_display_mode`, `hmi_static_text_1` and `hmi_static_text_2` triggers a write access to non-volatile memory with a limited number of write-cycles, it is strongly recommended to write these parameters only if necessary.

Command example

Query for selecting the display mode `static_text`:

```
http://<IP address>/cmd/set_parameter?hmi_display_mode=static_text
```

Query for setting the displayed text to 'Hello World':

```
http://<IP address>/cmd/set_parameter?hmi_static_text_1=Hello&hmi_static_text_2=World!
```

4.2.3 Dynamic text messages (application text)

The display mode `application_text` enables client applications to display up to two lines of custom text on the HMI LED display. The application text lines are stored in the parameters `hmi_application_text_1` and `hmi_application_text_2` using volatile memory only, i.e. the content is lost during reset. Therefore, this display mode is especially suited for displaying frequently updated information, e.g. status information of the client application processing the sensors scan data. Per default (e.g. after power-on) `hmi_application_text_1` and `hmi_application_text_2` are empty.

Steps for displaying application text messages are:

1. Enable the application text display by setting parameter `hmi_display_mode` to `application_text` using `set_parameter`.
2. Write text for the upper display line to `hmi_application_text_1` using `set_parameter`.
3. Write text for the lower display line to `hmi_application_text_2` using `set_parameter`.

Please note:

Since each write access to `hmi_display_mode` triggers a write access to non-volatile memory with a limited number of write-cycles, it is strongly recommended to write it only to select the display mode. For subsequent content updates write to `hmi_application_text_1` and `hmi_application_text_2` only.

Command example

Query for selecting the display mode `application_text`:

```
http://<IP address>/cmd/set_parameter?hmi_display_mode=application_text
```

Query for setting the displayed text to '*My status message*':

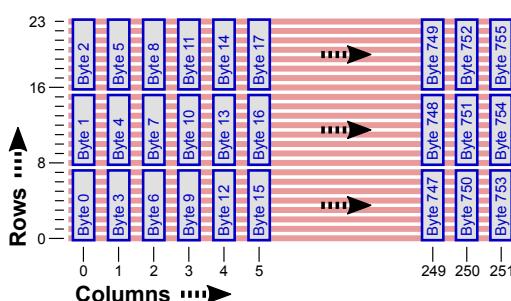
```
http://<IP address>/cmd/set_parameter?hmi_application_text_1=My status&hmi_application_text_2=message
```

4.3 Displaying custom bitmaps

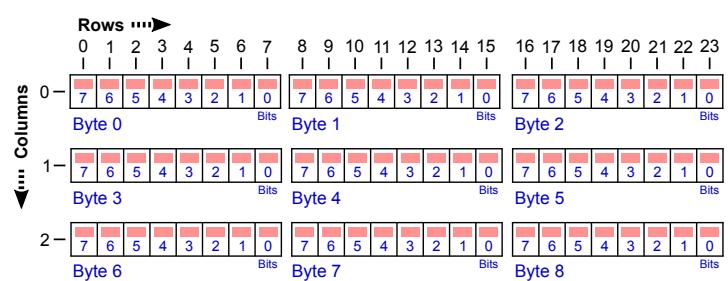
Alternatively to simple text messages (as described in section 4.2) the sensor allows client application to display custom bitmaps on the HMI LED display. This gives maximum flexibility regarding the displayed content, but requires more complex preparations by the client firmware. Similar to the display modes for text messages the sensor provides a mode for static bitmaps (logos) that are preserved even after a power-cycle and a mode for rather dynamic graphics that are updated by the client application more frequently.

4.3.1 Overview

Section 4.1 did already cover various details on the technical implementation of the LED display. This section concentrates on how display pixels are mapped into a binary frame buffer and how this data is transferred to the sensor.



(a) Mapping of bitmap to bytes



(b) Mapping of pixels to bytes

Figure 4.3: Byte mapping of HMI display pixels

Figure 4.3 shows the mapping of display pixels to a binary frame buffer. Each pixel of the LED display (see fig. 4.2) is represented by a single bit within this frame buffer. The 6048 pixels ($24 * 252 = 6048$) of a complete display image map into a frame buffer of 756 B ($6048/8 = 756$). The mapping starts at row 0 of column 0 in the lower left corner of the 2D display image: Pixel (0;0) maps into byte 0 bit 7, pixel (0;1) maps into byte 0 bit 6 and so on. The last pixel (0;23) of the first column maps into byte 3 bit 0. The first pixel (1;0) of the second column maps into byte 4 bit 7. This mapping scheme

continues column by column until the very last pixel (251; 23) in the upper right corner of the 2D display image fills bit 0 of byte 755.

Bitmap access to the HMI LED display always updates the complete display frame buffer. The necessary data is stored in binary form within the display parameters `hmi_static_logo` and `hmi_application_bitmap` – see subsequent sections for details. Writing to these parameters with `set_parameter` requires the binary content to be encoded as `base64url` string for the command URI (see sections 1.2.1 and 1.2.2). Reading the parameters returns a `base64` encoded string as part of the `JSON` encoded (see section 1.2.3). Please refer to section 2.1 for a more detailed description of binary parameter types.

4.3.2 Static bitmaps

The parameter `hmi_static_logo` allows to customize the graphic shown by the HMI display mode `static_logo`. The static bitmap is stored into non-volatile memory, i.e. the content is not lost during a power-cycle. Therefore, this display mode is especially suited for displaying rarely updated information, e.g. a custom company logo. The parameter `hmi_static_logo` is reset on request only (e.g. when loading the factory defaults). The default value shows a Pepperl+Fuchs logo.

Steps for customizing the static logo are:

1. Write a custom bitmap to `hmi_static_logo` using `set_parameter`.
2. Display the bitmap by setting parameter `hmi_display_mode` to `static_logo` using `set_parameter`.

Please note:

Since each write access to `hmi_display_mode` and `hmi_static_logo` triggers a write access to non-volatile memory with a limited number of write-cycles, it is strongly recommended to write these parameters only if necessary.

4.3.3 Application bitmaps

The display mode `application_bitmap` enables client applications to display a custom bitmap image on the HMI LED display. The bitmap is stored in the parameter `hmi_application_bitmap` using volatile memory only, i.e. the content is lost during reset. Therefore, this display mode is especially suited for displaying frequently updated information, e.g. status graphics of the client application processing the sensors scan data. Per default (e.g. after power-on) `hmi_application_bitmap` is empty.

Steps for displaying an application bitmap are:

1. Switch the display mode to Display the bitmap by setting parameter `hmi_display_mode` to `static_logo` using `set_parameter`.
2. Write the application bitmap to parameter `hmi_application_bitmap` using `set_parameter`.

Please note:

Since each write access to `hmi_display_mode` triggers a write access to non-volatile memory with a limited number of write-cycles, it is strongly recommended to write it only to select the display mode. For subsequent content updates write to `hmi_application_bitmap` only.

Please note:

The interface to the HMI LED display is currently not designed for real-time updates. It is recommended to update the application bitmap not more often than once per second (update rate 1 Hz). In case of faster updates the behavior of the display is undefined.

4.3.4 Converting graphics for the HMI display

To convert an existing graphic to the HMI LED display the following steps are recommended:

1. Stretch the graphic by factor 3 in horizontal direction to compensate for the asymmetrical display resolution.
2. Trim the image to an aspect ratio of 2 : 21 (vertical:horizontal). Keep in mind that the image is shown on a 360 degree surface, so repeating the image for different view angles might be a good idea. A tried and trusted approach is to trim the image to a 2 : 7 aspect ration and then repeat this image three times in horizontal direction.
3. Down-scale the image to a resolution of 24 x 252 pixels.
4. Reduce the image to a black-and-white graphics with only two colors.
5. If necessary, manually optimize the resulting low-resolution graphic by removing artifacts from the conversion process.

6. Save the image to a common graphics file format with support for monochrome images (2 bits per pixel).
7. Convert the image file to binary format using a common image conversion tool like [Image Magick](#). The following command uses the tool `convert` from *Image Magick* to convert a bitmap into the correct raw binary data:

```
> convert input.bmp -rotate 90 -negate GRAY:output.bin
```

The resulting binary file ('output.bin' in the above example) should have a size of exactly 756 B.

8. Finally, store the binary data in either `hmi_static_logo` or `hmi_application_bitmap`. The data needs to be encoded as base64url string [8] with a length of exactly 1008 B.

It is highly recommended to use vector graphics as source for creating bitmaps for the HMI LED display. This way many conversion artefacts can be avoided resulting in higher image quality.

5 Advanced topics

This chapter covers various advanced topics about using R2000 devices in more complex applications.

5.1 Device discovery using SSDP

The R2000 provides support for the *Simple Service Discovery Protocol (SSDP)* [13] in order to discover any R2000 devices and their associated IP address within the Ethernet network. SSDP uses UDP multicast messages to query SSDP aware devices.

In order to discover all R2000 devices, the following steps need to be performed:

1. Send a SSDP search request.
2. Process SSDP replies from devices.
3. Read a SSDP device description from each device for additional information.

The following sections describe each step in detail.

5.1.1 SSDP search request

The first step of the SSDP device discovery is to issue a search request on the local network. For this purpose an UDP listener needs to be opened on the local UDP port 1900. Then an UDP datagram with the following content needs to be sent to the UDP multicast address 239.255.255.250 at port 1900:

```

1 M-SEARCH * HTTP/1.1
2 HOST: 239.255.255.250:1900
3 ST: urn:pepperl-fuchs-com:device:R2000:1
4 MAN: "ssdp:discover"
5 MX: 1

```

The specified URN addresses R2000 devices only. Other SSDP aware devices on the network will ignore this request.

Please note:

On a client PC with multiple network adapters, the SSDP search request needs to be performed on each network adapter.

5.1.2 SSDP device reply

The second step of the discovery procedure requires the client application to wait for replies to the above search request using the created UDP listener. Each R2000 device on the local network will answer the search request with a message similar to this example:

```

1 HTTP/1.1 200 OK
2 LOCATION: http://10.0.10.9/ssdp.xml
3 SERVER: pfda/1.0 UPnP/1.0 R2000/1.0
4 CACHE-CONTROL: max-age=1800
5 EXT:
6 ST: urn:pepperl-fuchs-com:device:R2000:1
7 USN: uuid:7df9a5ed-07f6-45e1-ac55-333340704340::urn:pepperl-fuchs-com:device:R2000:1

```

This reply contains two important pieces of information:

- The line `LOCATION:` contains the IP address of the device within an URL pointing to a more detailed SSDP device description (see next section).
- The line `USN:` contains an unique identifier (uuid) for this specific device. This uuid allows to identify this R2000 device even if its IP address changes.



5.1.3 SSDP device description

The final step of the SSDP discovery procedure is to obtain the XML based device description. This step can be skipped, if no detailed information on the discovered devices are needed. R2000 devices provide a `ssdp.xml` file at the URL from the `LOCATION` field of the SSDP device reply (see previous section):

```
1 <?xml version="1.0"?>
2 <root xmlns="urn:schemas-upnp-org:device-1-0">
3   <specVersion>
4     <major>1</major>
5     <minor>0</minor>
6   </specVersion>
7   <device>
8     <deviceType>urn:pepperl-fuchs-com:device:R2000:1</deviceType>
9     <friendlyName>OMD10M-R2000-B23-V1V1D (#40000007343704)</friendlyName>
10    <manufacturer>Pepperl+Fuchs</manufacturer>
11    <manufacturerURL>http://www.pepperl-fuchs.com</manufacturerURL>
12    <modelDescription>2D Laser Scanner</modelDescription>
13    <modelName>OMD10M-R2000-B23-V1V1D</modelName>
14    <modelNumber>232934</modelNumber>
15    <serialNumber>40000007343704</serialNumber>
16    <UDN>uuid:7df9a5ed-07f6-45e1-ac55-333340704340</UDN>
17    <serviceList>
18      <service>
19        <serviceType>urn:pepperl-fuchs-com:service:none:1</serviceType>
20        <serviceId>urn:pepperl-fuchs-com:serviceId:none</serviceId>
21        <controlURL>/cmd/</controlURL>
22        <eventSubURL></eventSubURL>
23        <SCPDURL>/service.xml</SCPDURL>
24      </service>
25    </serviceList>
26    <iconList>
27      <icon>
28        <id>0</id>
29        <mimetype>image/png</mimetype>
30        <width>48</width>
31        <height>48</height>
32        <depth>24</depth>
33        <url>/device.png</url>
34      </icon>
35    </iconList>
36    <X_pfsdpVersionMajor>1</X_pfsdpVersionMajor>
37    <X_pfsdpVersionMinor>2</X_pfsdpVersionMinor>
38    <X_pfsdpDeviceFamily>1</X_pfsdpDeviceFamily>
39    <X_dtmAccessPath>/dtm/</X_dtmAccessPath>
40  </device>
41 </root>
```

The standard SSDP XML device description contains already various useful fields:

- `manufacturer` – vendor name of the device (see parameter `vendor` in section 2.3)
- `modelName` – product name of the device (see parameter `product` in section 2.3)
- `modelNumber` – part number of the device (see parameter `part` in section 2.3)
- `serialNumber` – serial number of the device (see parameter `serial` in section 2.3)

R2000 devices additionally provide the following non-standard items with PFSDP specific information:

- `X_pfsdpVersionMajor` – major PFSDP protocol revision (see `version_major` in section 1.2.7)
- `X_pfsdpVersionMinor` – minor PFSDP protocol revision (see `version_minor` in section 1.2.7)
- `X_pfsdpDeviceFamily` – PFSDP device family (see `device_family` in section 2.3)



A Troubleshooting the Ethernet communication

This chapter contains some basic suggestions for troubleshooting issues concerning the R2000 Ethernet communication.

A.1 Checking the Ethernet setup

In case of communication problems, first ensure a working Ethernet connection between PC and sensor. Please consider the following steps:

- **Sensor IP configuration**

Check the current IP configuration of the Sensor in the HMI menu "Ethernet Info" (see user manual). If necessary, change the configuration in the "Ethernet Setup" menu and reboot the device to apply the changes. Now verify the IP configuration in the "Ethernet Info" menu.

- **Ethernet connection**

Use the network utility *ping* to verify the network connection between sensor and PC. The sensor will reply to all ping requests it receives. If *ping* does not receive any replies, re-check the IP configuration of your client PC and the sensor. Make sure the IP addresses of both devices are within the same subnet.

- **Electrical connection**

In case of connectivity problems, check the link status and link speed of the sensor, the client PC and any network infrastructure device (router, switch, etc.) in-between to rule out electric connection issues. For maximum reliability, try to use a direct cable-based Ethernet connection between sensor and PC. The sensor supports Auto-MDIX – a cross-over Ethernet cable is not required.

A.2 Debugging using a web browser

If basic network connectivity has been established, verify that the HTTP command interface is operational with a standard web browser. Please consider these steps:

- **Proxy settings**

Make sure that no proxy is used when accessing the sensor. In the browser settings, either completely disable any proxy or add a proxy exception for the sensor IP address.

- **HTTP access**

Try to access the sensor via the following URL:

```
http://<sensor IP address>/cmd/protocol_info
```

This command should return some basic protocol information (see section 1.2.7). If this is not the case, re-check your proxy settings and Ethernet setup (see above).

- **HTTP commands**

You can test the syntax and effect of any HTTP command used in your application software just by sending the command from a web browser. The web browser will display the response received from the sensor – making it easy to review any potential error messages. Furthermore, after changing sensor settings with the `set_parameter` command (see section 2.2.3), it might be helpful to read back all parameters using the command `get_parameter` (see section 2.2.2).

A.3 Debugging using Wireshark

For complex communication issues it is highly recommended to use the free network traffic analysis tool *Wireshark* [12] to sniff and record the Ethernet communication between the client software and the R2000 sensor.



For example, this can be very helpful for:

- Checking the content of HTTP messages and the corresponding replies
- Checking order and time behavior of HTTP commands
- Checking time behavior of scan data output (TCP or UDP)

In case you contact your sensor support representative about a specific communication issue, it is highly recommended to have a Wireshark log file (.pcap) at hand for examination by the technical support organisation.



B Protocol version history

B.1 Protocol version 1.02 (R2000 firmware v1.21 or newer)

Minor protocol extensions (backward-compatible to protocol versions 1.00 and 1.01)

Notable extensions:

- Section 2.4: Added new informational parameter `emitter_type`.
- Section 2.6.5: Added scan resolutions 1680, 2100 and 2800 to R2000 UHD and HD devices (Table 2.1).

B.2 Protocol version 1.01 (R2000 firmware v1.20 or newer)

Protocol enhancements (backward-compatible to protocol version v1.00)

Significant extensions:

- Section 2.7: Added access to bitmap shown by display mode `static_logo`
- Section 2.7: Added display mode `static_text` to show static custom text
- Section 2.7: Added display mode `application_bitmap` to show a dynamic custom bitmap
- Section 2.7: Added display mode `application_text` to show a dynamic custom text
- Section 3.2.4: Added option `max_num_points_scan` to limit number of points per scan for scan data output
- Section 3.3.9: Added mechanism for TCP in-line watchdog feeds

Notable extensions:

- Section 2.2.6: Added new command `factory_reset` to perform a complete factory reset.
- Section 2.3: Added device family for HD devices (OMDxxx-R2000-HD)
- Section 2.4: Added capability values `scan_frequency_min` and `scan_frequency_max`
- Section 2.4: Added capability values `sampling_rate_min` and `sampling_rate_max`
- Section 2.6.2: Added parameter `operating_mode` to control mode of operation (e.g. disable emitter)
- Section 2.7: Added new parameter `hmi_parameter_lock` for setting the HMI menu to read-only.
- Section 3.4.2: Redefined field `output_status` to `iq_input` (all scan data packet headers)
- Section 3.4.2: Redefined field `field_status` to `iq_overload` (all scan data packet headers)

B.3 Protocol version 1.00 (R2000 firmware v1.00 or newer)

First public release.



C Document change history

C.1 Release 2016-03 (protocol version 1.02)

Minor documentation update for protocol version 1.02:

- Section 2.6.5: Added list of available scan resolutions for R2000 HD devices to table 2.1.
- Section 3.4.3: Updated description of flag `new_settings`.
- Section 5.1: Added section on device discovery using SSDP.
- Various textual and cosmetic updates

C.2 Release 2015-04 (protocol version 1.01)

Document update for protocol version 1.01:

- Added descriptions for all protocol extensions listed in appendix B.2
- Section 1.2.2: Moved description of parameter types to separate section (section 2.1)
- Section 2.1: Extended description for various parameter types (`bitfield`, `string`, `IPv4`, `ntp64`, `binary`)
- Section 2.8.2: Added missing description of temperature warning and error flags in system status flags
- Section 3.2: Separated description of basic scan data output mechanisms from description of commands (section 3.3)
- Section 3.2.2: Added separate section for details on connection handles and backwards compatibility
- Section 3.2.3: Added separate section for details on the connection watchdog mechanism
- Section 3.2.4: Added section on configuration options for scan data output
- Section 3.2.5: Added separate section on performance considerations for concurrent scan data connections
- Section 3.4.3: Added missing description of temperature warning and error flags in scan data header status flags
- Chapter 4: Added chapter about client application access to the HMI LED display
- Appendix B: Separated protocol history and document history
- Various textual and cosmetic updates

C.3 Release 2013-08 (protocol version 1.00)

First public release.



Index for commands and parameters

This index provides a quick reference for all commands and parameters defined by this communication protocol.

Generic commands (URI)

factory_reset, 15, 55
feed_watchdog, 30, 37, 38
get_parameter, 13, 17, 28, 53
get_protocol_info, 8
get_scanoutput_config, 36, 37
list_parameters, 13
reboot_device, 15, 19
release_handle, 35
request_handle_tcp, 30, 33, 34
request_handle_udp, 30, 32
reset_parameter, 14, 15, 19
set_parameter, 14, 15, 19, 29, 36, 47–49, 53
set_scanoutput_config, 30, 32, 33, 36, 38
start_scanoutput, 35, 36
stop_scanoutput, 35, 36

Global parameters (sensor)

angular_fov, 18
angular_resolution, 18
contamination, 24
deprecated_handle_generation, 29
device_family, 17
emitter_type, 18, 55
feature_flags, 18
gateway, 19
gateway_current, 19
hmi_application_bitmap, 22, 49, 50
hmi_application_text_1, 22, 48
hmi_application_text_2, 22, 48
hmi_button_lock, 22, 23
hmi_display_mode, 22, 23, 25, 47–49
hmi_language, 22, 23
hmi_parameter_lock, 22, 23, 55
hmi_static_logo, 22, 49
hmi_static_logo], 50
hmi_static_text_1, 22, 47
hmi_static_text_2, 22, 47
ip_address, 19
ip_address_current, 19
ip_mode, 19
ip_mode_current, 19
load_indication, 24, 25, 31
locator_indication, 22, 23
mac_address, 19
max_connections, 18, 31
max_data_regions, 18
max_scan_sectors, 18
operating_mode, 20, 55
operation_time, 24
operation_time_scaled, 24
part, 17, 52
power_cycles, 24
product, 17, 52
radial_range_max, 18, 27

radial_range_min, 18, 27
radial_resolution, 18, 27
revision_fw, 17
revision_hw, 17
samples_per_scan, 20–22, 26, 30, 40–44
sampling_rate_max, 18, 21, 55
sampling_rate_min, 18, 21, 55
scan_direction, 20, 21, 46
scan_frequency, 20, 21, 26, 46
scan_frequency_max, 18, 55
scan_frequency_measured, 20
scan_frequency_min, 18, 55
serial, 17, 52
status_flags, 24
subnet_mask, 19
subnet_mask_current, 19
system_time_raw, 24, 28
temperature_current, 24
temperature_max, 24
temperature_min, 24
up_time, 24
user_notes, 17
user_tag, 17
vendor, 17, 52

Scan data output parameters

address, 32–34
handle, 6, 32, 33, 35–37
max_num_points_scan, 30, 32, 33, 36, 40, 42–44, 55
packet_type, 32, 33, 36
port, 32–34
start_angle, 30, 32, 33, 36
watchdog, 30, 32, 33, 36, 38
watchdogtimeout, 30, 32, 33, 36, 38



References

- [1] RFC-791: Internet Protocol Specification
<http://tools.ietf.org/html/rfc791>
- [2] RFC-1305: Network Time Protocol (Version 3)
<http://tools.ietf.org/html/rfc1305>
- [3] RFC-2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
<http://tools.ietf.org/html/rfc2046>
- [4] RFC-2616: Hypertext Transfer Protocol – HTTP/1.1
<http://tools.ietf.org/html/rfc2616>
- [5] RFC-2617: HTTP Authentication: Basic and Digest Access Authentication
<http://tools.ietf.org/html/rfc2617>
- [6] RFC-3629: UTF-8, a transformation format of ISO 10646
<http://tools.ietf.org/html/rfc3629>
- [7] RFC-3986: Uniform Resource Identifier (URI)
<http://tools.ietf.org/html/rfc3986>
- [8] RFC-4648: The Base16, Base32, and Base64 Data Encodings
<http://tools.ietf.org/html/rfc4648>
- [9] RFC-7159: The JavaScript Object Notation (JSON) Data Interchange Format
<http://tools.ietf.org/html/rfc7159>
- [10] Libwww: the W3C Protocol Library
<http://www.w3.org/Library/>
- [11] libcurl: free and easy-to-use client-side URL transfer library
<http://curl.haxx.se/libcurl/>
- [12] Wireshark: free network protocol analyzer for Unix and Windows
<http://www.wireshark.org/>
- [13] Simple Service Discovery Protocol (Draft v1.03)
<https://tools.ietf.org/html/draft-cai-ssdp-v1-03>
- [14] Zero Configuration Networking (Zeroconf)
<http://www.zeroconf.org/>

FACTORY AUTOMATION – SENSING YOUR NEEDS



Worldwide Headquarters

Pepperl+Fuchs GmbH · Mannheim · Germany
E-mail: fa-info@pepperl-fuchs.com

USA Headquarters

Pepperl+Fuchs Inc. · Twinsburg, OH · USA
E-mail: fa-info@us.pepperl-fuchs.com

Asia Pacific Headquarters

Pepperl+Fuchs Pte Ltd · Singapore
Company Registration No. 199003130E
E-mail: fa-info@sg.pepperl-fuchs.com

www.pepperl-fuchs.com

 **PEPPERL+FUCHS**
SENSING YOUR NEEDS

Subject to modifications without notice
Copyright Pepperl+Fuchs · Printed in Germany