DRIFT Protocol Specification

DRIFT (Driftveil Revolutionary Industrial Field Toolkit) is a custom industrial control systems (ICS) protocol used by Driftveil to securely get values and alarms from a PLC and its sensors.

Similar to other ICS protocols such as Modbus and BACnet, DRIFT is a request-response protocol. The PLCs only send DRIFT-RESPONSE messages as a response to DRIFT-REQUEST messages, they never initiate a connection or send other messages.

Cryptography

To protect data-in-motion, the DRIFT protocol uses AES-ECB 128-bit encryption (BLOCK-SIZE 16) for all messages after its initial new connection messages (NEW-CONNECTION-REQUEST / NEW-CONNECTION-RESPONSE). DRIFT uses the default AES padding PKCS7.

In order for an HMI to communicate with a PLC, it first needs to send a NEW-CONNECTION-REQUEST message. Upon receiving a NEW-CONNECTION-REQUEST message, the PLC will generate an 8 byte (64-bit) partial key and send the partial key back to the HMI within the NEW-CONNECTION-RESPONSE message. The PLC and HMI must save this partial AES key to encrypt/decrypt all other DRIFT messages within this session.

All other DRIFT messages must contain an 8 byte (64-bit) partial AES key. The remaining data in the DRIFT message must be encrypted by using both the saved partial key from the NEW-CONNECTION handshake and the partial key included in the message.

Message Types

Message Code	Message
0x01	NEW-CONNECTION
0x03	READ-SENSOR
0x04	READ-ALL-SENSORS
0x05	WRITE-SENSOR
0x06	GET-SENSOR-RANGES
0x07	GET-ALARMS

NEW-CONNECTION (Service Code - 0x01)

When a Driftveil HMI wants to communicate with a Driftveil PLC, the first message it sends is a NEW-CONNECTION-REQUEST message. The PLC will then respond with a NEW-CONNECTION-RESPONSE message that includes a partial AES key to be used for the remainder of the communication between that HMI and PLC.

NEW-CONNECTION-REQUEST

Field Name	Number of Bytes
Data length	2
Message code (NEW-CONNECTION)	1

NEW-CONNECTION-RESPONSE (Success)

Field Name	Number of Bytes
Data length	2
Message code (NEW-CONNECTION)	1
Response code (Success)	1
Partial AES Key	8

NEW-CONNECTION-RESPONSE (ERROR)

Field Name	Number of Bytes
Data length	2
Message code (NEW-CONNECTION)	1
Response code (Error code)	1

READ-SENSOR (Service Code - 0x03)

The READ-SENSOR message is used to read the value of a single sensor from a Driftveil PLC. The READ-SENSOR-REQUEST message indicates a single sensor ID it would like to read the value from. If successfully able to read the value of the sensor, the READ-SENSOR-RESPONSE contains the value of that sensor.

READ-SENSOR-REQUEST

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (READ-SENSOR)	1
Sensor ID	1

READ-SENSOR-RESPONSE (Success)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (READ-SENSOR)	1
Response code (Success)	1
Sensor ID	1
Value	4

READ-SENSOR-RESPONSE (ERROR)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (READ-SENSOR)	1
Response code (Error code)	1

READ-ALL-SENSOR (Service Code - 0x04)

The READ-ALL-SENSOR message is used to read the current values of all sensors from a Driftveil PLC. The READ-ALL-SENSOR-RESPONSE message contains the sensor IDs and current values for all PLC sensors.

READ-ALL-SENSOR-REQUEST

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (READ-ALL-SENSOR)	1

READ-ALL-SENSOR-RESPONSE (Success)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (READ-ALL-SENSOR)	1
Response code (Success)	1
Sensor count	1
List of SENSOR-VALUES	5 * Sensor count

SENSOR-VALUES

Field Name	Number of Bytes
Sensor ID	1
Value	4

READ-ALL-SENSOR-RESPONSE (ERROR)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (READ-ALL-SENSOR)	1
Response code (Error code)	1

WRITE-SENSOR (Service Code - 0x05)

The WRITE-SENSOR message is used to set the value of a single sensor on a Driftveil PLC. The WRITE-SENSOR-REQUEST message indicates a single sensor ID and value to set the sensor to. The WRITE-SENSOR-RESPONSE contains a response code, indicating if the write was successful.

WRITE-SENSOR-REQUEST

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (WRITE-SENSOR)	1
Sensor ID	1
Value	4

WRITE-SENSOR-RESPONSE (Success)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (WRITE-SENSOR)	1
Response code (Success)	1

WRITE-SENSOR-RESPONSE (ERROR)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (WRITE-SENSOR)	1
Response code (Error code)	1

GET-SENSOR-RANGES (Service Code - 0x06)

The GET-SENSOR-RANGES message is used to get the normal, warning, and alert operating ranges for the sensor IDs provided in the GET-SENSOR-RANGES-REQUEST. The GET-SENSOR-RANGES-RESPONSE contains the WARNING-LOW, WARNING-HIGH, ALERT-LOW, and ALERT-HIGH values for each sensor listed in the request.

GET-SENSOR-RANGES-REQUEST

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (GET-SENSOR-RANGES)	1
Sensor count	1
List of sensor IDs	1 * Sensor count

GET-SENSOR-RANGES-RESPONSE (Success)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (GET-SENSOR-RANGES)	1
Response code (Success)	1
Sensor count	1
List of SENSOR-RANGES	17 * Sensor count

SENSOR-RANGES

Field Name	Number of Bytes
Sensor ID	1
Sensor range - WARNING-LOW	4
Sensor range - WARNING-HIGH	4
Sensor range - ALERT-LOW	4
Sensor range - ALERT-HIGH	4

GET-SENSOR-RANGES-RESPONSE (ERROR)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8

Field Name	**Number of Bytes**
Message code (GET-SENSOR-RANGES)	1
Response code (Error code)	1

GET-ALARMS (Service Code - 0x07)

The GET-ALARMS message is used to get all active warnings and alerts from a Driftveil PLC.

GET-ALARMS-REQUEST

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (GET-ALARMS)	1

GET-ALARMS-RESPONSE (Success)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (GET-ALARMS)	1
Response code (Success)	1
Alarm count	1
List of ALARM-DATA	6 * Alarm count

ALARM-DATA

Field Name	Number of Bytes
Sensor ID	1
Alarm code	1
Value	4

GET-ALARMS-RESPONSE (ERROR)

Field Name	Number of Bytes
Data length	2
Partial AES Key	8
Message code (GET-ALARMS)	1
Response code (Error code)	1

Appendix

Message Codes

Message Code	Message
0x01	NEW-CONNECTION
0x03	READ-SENSOR
0x04	READ-ALL-SENSORS
0x05	WRITE-SENSOR
0x06	GET-SENSOR-RANGES
0x07	GET-ALARMS

Response Codes

Response Code	Response Code Description
0x00	Operation was successful
0x01	ERROR: Connection already exists
0x02	ERROR: Invalid message format
0x03	ERROR: Sensor not found
0x04	ERROR: Sensor not writeable
0x05	ERROR: Invalid message length
0x06	ERROR: Server error
0x07	ERROR: Unknown command
0x08	ERROR: Encryption key not initialized
0xfe	ERROR: Not authorized

Alarm Codes

Alarm Code	Alarm Description
0xa0	WARNING: LOW
0xa1	WARNING: HIGH
0xb0	ALERT: LOW
0xb1	ALERT: HIGH