Modbus Communication Basics

EXTREME TELEMATICS CORP.

Overview

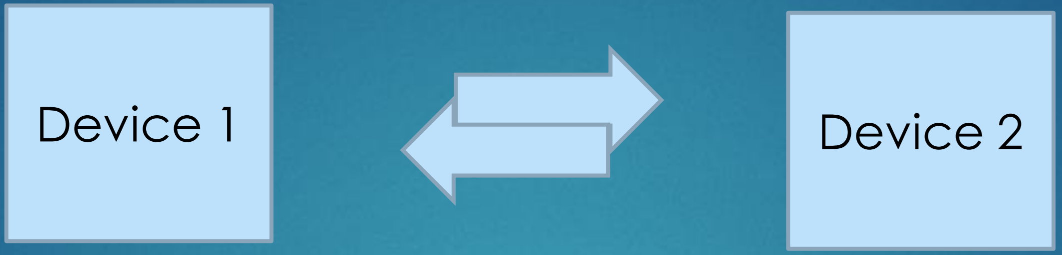
- Open Systems Interconnection (OSI) Model
- Physical Interfaces
- Modbus Protocol
  - Master/Slave Relationship
  - Data Frames
  - Register Types
  - Function Codes
- Examples

Open Systems Interconnection (OSI) Model

- 7. Application Layer – High level APIs, resource sharing
- 6. Presentation Layer – Translation of data
- 5. Session Layer – Management of communication sessions
- 4. Transport Layer – Reliable transmission between points
- 3. Network Layer – Addressing and routing on multi-node network
- 2. Data Link Layer – Reliable transmission of data frames
- 1. Physical Layer – Transmission of raw bits

Layer 1 – Physical Layer

Transceivers



- This is like placing a phone call, but not setting the language or speed of the voice
- Transceiver chip on the circuit board

RS-232

- Serial data transmission
- 9 pin connector
- Rarely in new devices

RS-485

- Serial data transmission
- 2 wire differential with ground
- Longer distance + multi drop

USB

- Serial data transmission
- Higher speed/power
- Power delivery

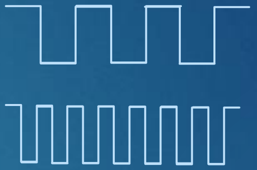
Ethernet

- IP based communication
- Higher speed/power
- Power delivery (POE)

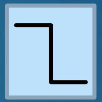
ETC
EXTREME TELEMATICS CORP.

Serial Communications

- Baud Rate
  - How fast the data is transmitted. Bits per second (bps)
  - Common rates are 2400, 9600, 19.2k, 38.4k, 57.6k, 115.2k



- Start Bit
  - Indicates the start of transmission



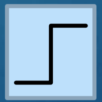
- Data Bits
  - Number of bits sent per transmission
  - Typically 7 (ASCII) or 8 (Equal to a byte). Can be 5 to 9.

D0 • • • Dx

- Parity
  - Error detection method
  - Typically set to None. Can also be Odd, Even, Mark (1), or Space (0)

P

- Stop Bits
  - Number of bits to indicate the end of character
  - Typically 1. Can also be 1.5 or 2

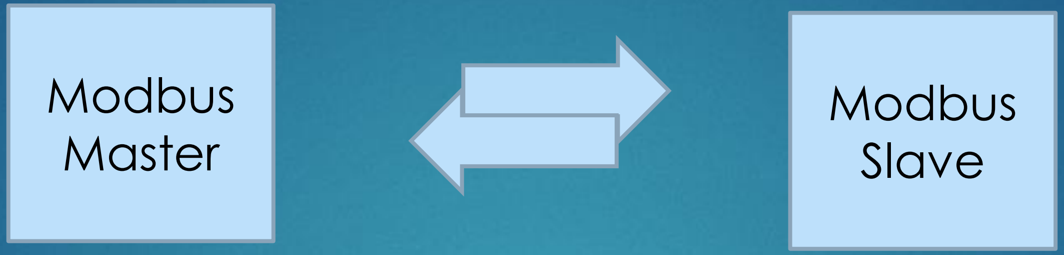


Example: 9600 8N1

Start	D0	D1	D2	D3	D4	D5	D6	D7	P	Stop

Layer 2 – Data Link Layer

Modbus Overview



- Poll/response protocol
- Master station interacts with slave nodes in a round robin fashion
- Two different formats for data transport
  - ASCII – Data represents characters i.e. 18095 sent as 5 characters/bytes, “1”, “8”, …
  - RTU – Data is binary. i.e. 18095 sent as 2 bytes (16 bits)
- Max message size 256 bytes
- Valid addresses are 1 – 247
  - 0 reserved for broadcast messages
  - 248 – 255 are reserved

Modbus Messages - Serial

RTU

Name	Length (Bytes)	Function
Start	3.5	Minimum silence (mark condition)
Address	1	Station address
Function	1	Code that indicates data type and operation
Data	n x 1	Length + data
CRC	2	Cyclic redundancy check
End	3.5	Silence between frames

ASCII

Name	Length (Bytes)	Function
Start	1	Colon character
Address	2	Station address
Function	2	Code that indicates data type and operation
Data	n x 2	Length + data
LRC	2	Longitudinal Redundancy Check (Checksum)
End	2	Carriage return – Line feed characters

Modbus Messages - Ethernet

Name	Length (Bytes)	Function
Transaction Identifier	2	Synchronization between server and client
Protocol Identifier	2	0 for Modbus TCP
Length	2	Bytes remaining
Unit Identifier	1	Station Address
Function Code	1	Code that indicates data type and operation
Data Bytes	n	Data

Layer 3 – Network Layer

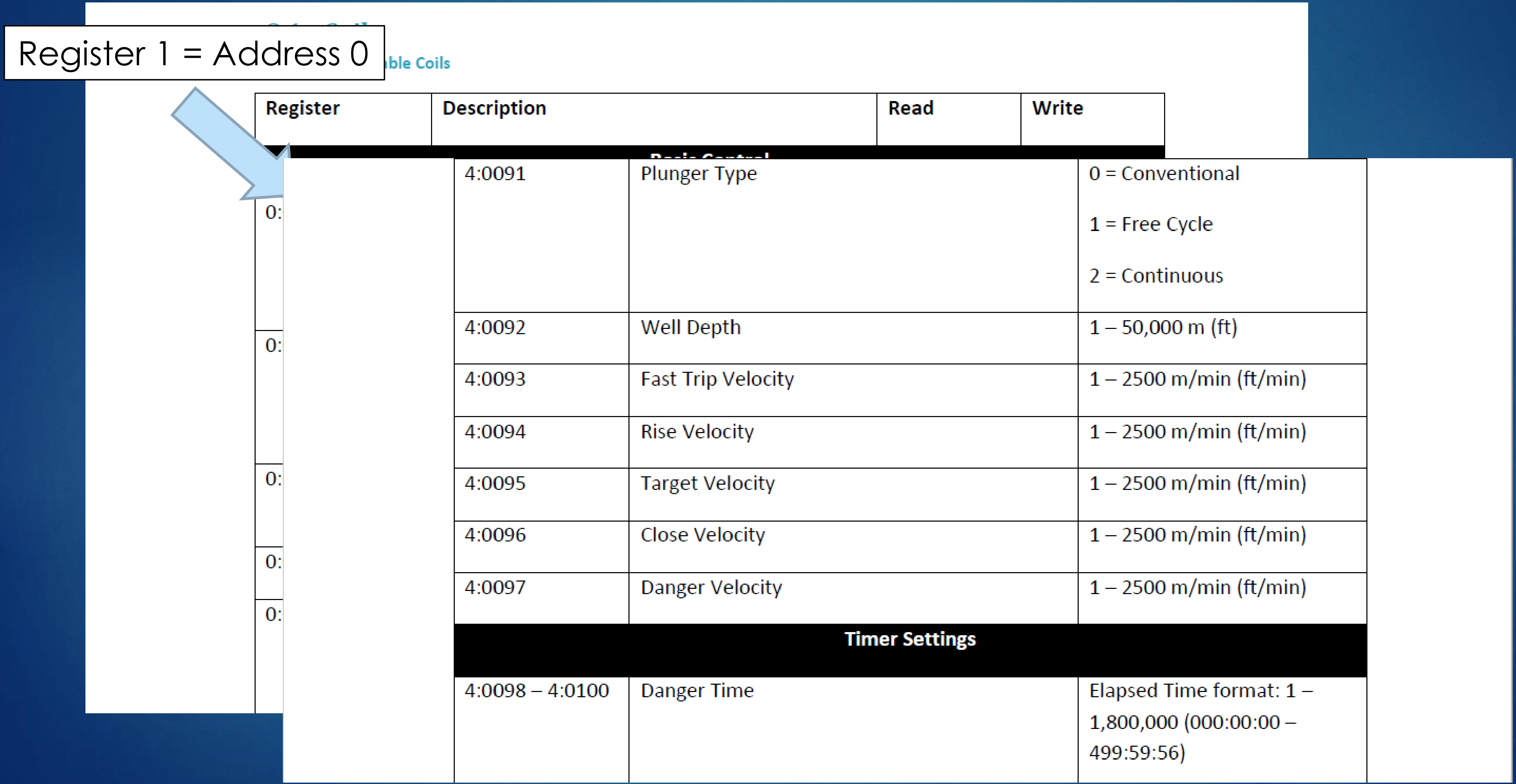
Modbus Data

- Overview
  - Data stored in coils/discretes (1 bit) or registers (16 bits)
  - Registers grouped by type of data
  - Each device type has a defined set of registers
  - No consistency between manufacturers
- Data Blocks
  - 0:xxxx – **Coils** – Read/write binary value (i.e. Valve Status)
  - 1:xxxx – **Input Discretes** – Read only input state (i.e. Line Pressure Switch)
  - 3:xxxx – **Input Registers** – Read only value (i.e. Line Pressure Sensor)
  - 4:xxxx – **Holding Registers** – Read/write value (i.e. Close Time)

Modbus Functions

- 01 – Read Coils
- 02 – Read Input Discretes
- 03 – Read Multiple Registers (Holding Registers)
- 04 – Read Input Registers
- 05 – Write Coil
- 06 – Write Single Register
- 15 – Force Multiple Coils
- 16 – Write Multiple Registers (Holding Registers)

ALiEn^2 Modbus Guide



Register 1 = Address 0

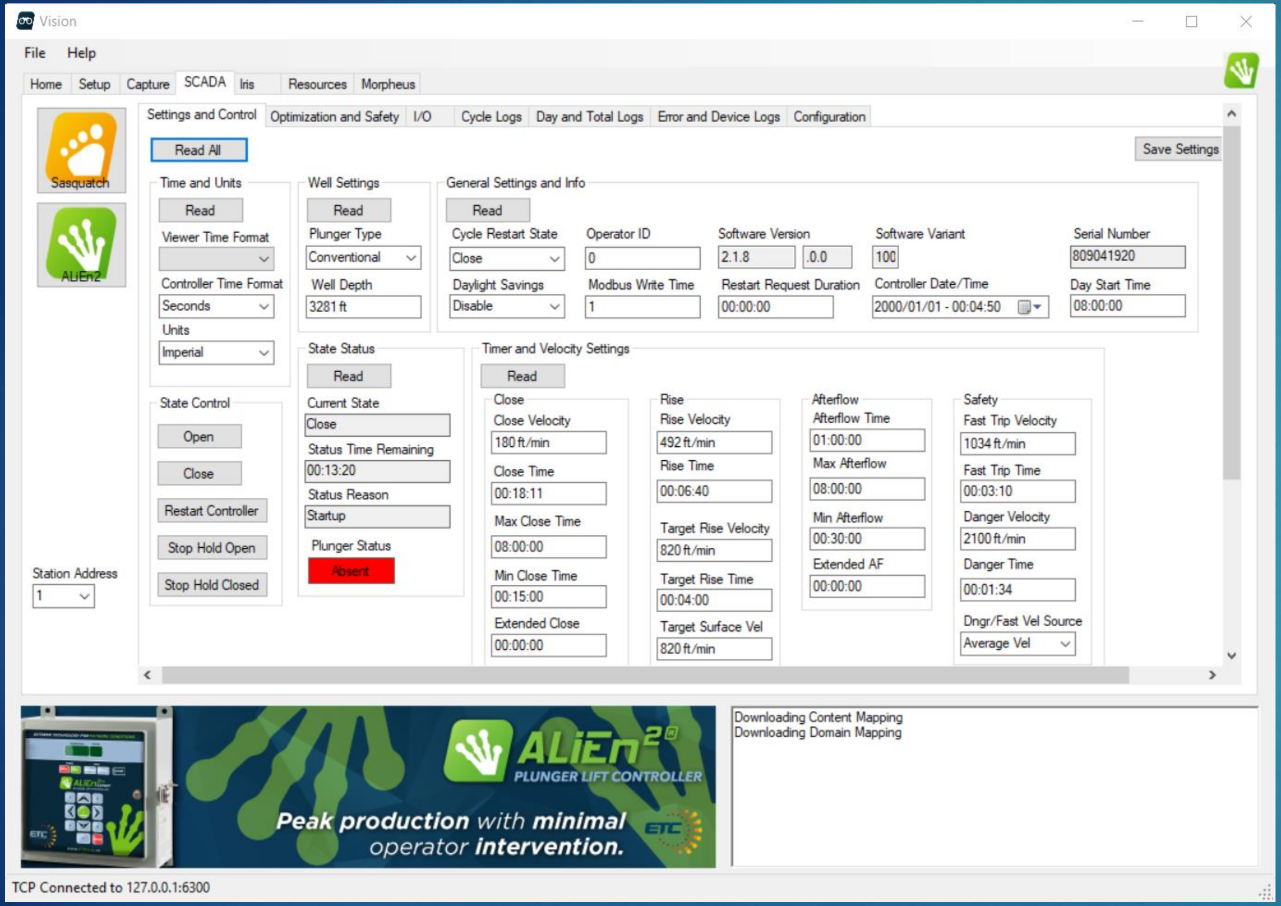
ble Coils

Register	Description	Read	Write
0:			
0:			
0:			
0:			
0:			

4:0091	Plunger Type	0 = Conventional 1 = Free Cycle 2 = Continuous
4:0092	Well Depth	1 – 50,000 m (ft)
4:0093	Fast Trip Velocity	1 – 2500 m/min (ft/min)
4:0094	Rise Velocity	1 – 2500 m/min (ft/min)
4:0095	Target Velocity	1 – 2500 m/min (ft/min)
4:0096	Close Velocity	1 – 2500 m/min (ft/min)
4:0097	Danger Velocity	1 – 2500 m/min (ft/min)
Timer Settings		
4:0098 – 4:0100	Danger Time	Elapsed Time format: 1 – 1,800,000 (000:00:00 – 499:59:56)

4/21/2020

Vision and ALiEn2 (RS-485)



Time and Units
- Read
- Viewer Time Format:
- Controller Time Format: Seconds
- Units: Imperial

Well Settings
- Read
- Plunger Type: Conventional
- Well Depth: 3281 ft

General Settings and Info
- Read
- Cycle Restart State: Close
- Operator ID: 0
- Software Version: 2.1.8 .0.0
- Software Variant: 100
- Serial Number: 809041920
- Daylight Savings: Disable
- Modbus Write Time: 1
- Restart Request Duration: 00:00:00
- Controller Date/Time: 2000/01/01 - 00:04:50
- Day Start Time: 08:00:00

State Control
- Open
- Close
- Restart Controller
- Stop Hold Open
- Stop Hold Closed

Station Address: 1

State Status
- Read
- Current State: Close
- Status Time Remaining: 00:13:20
- Status Reason: Startup
- Plunger Status: Absent

Timer and Velocity Settings
- Read

Close
- Close Velocity: 180 ft/min
- Close Time: 00:18:11
- Max Close Time: 08:00:00
- Min Close Time: 00:15:00
- Extended Close: 00:00:00

Rise
- Rise Velocity: 492 ft/min
- Rise Time: 00:06:40
- Target Rise Velocity: 820 ft/min
- Target Rise Time: 00:04:00
- Target Surface Vel: 820 ft/min

Afterflow
- Afterflow Time: 01:00:00
- Max Afterflow: 08:00:00
- Min Afterflow: 00:30:00
- Extended AF: 00:00:00

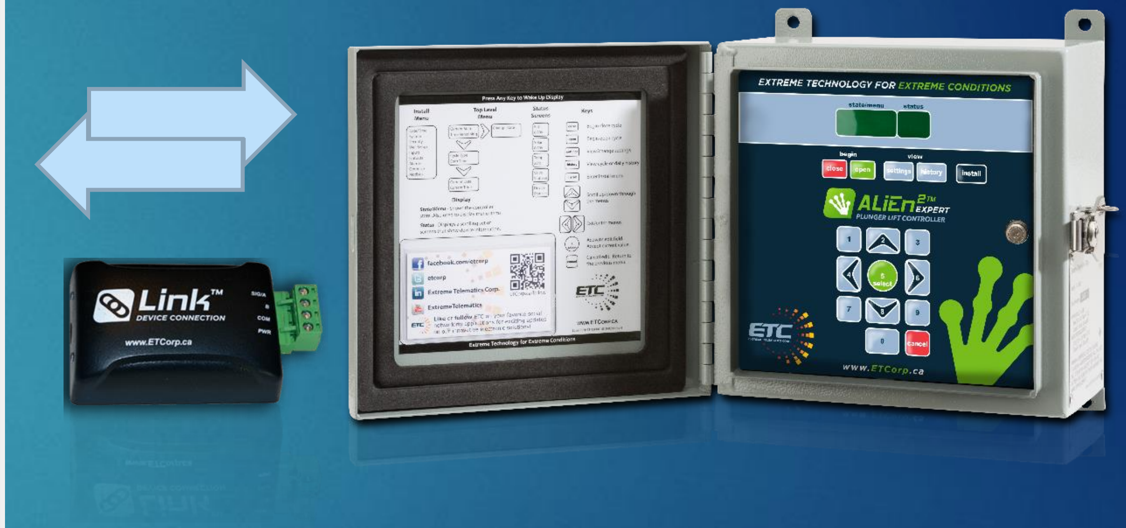
Safety
- Fast Trip Velocity: 1034 ft/min
- Fast Trip Time: 00:03:10
- Danger Velocity: 2100 ft/min
- Danger Time: 00:01:34
- Dngr/Fast Vel Source: Average Vel

```
Downloading Content Mapping
Downloading Domain Mapping
```

ALiEn2 PLUNGER LIFT CONTROLLER

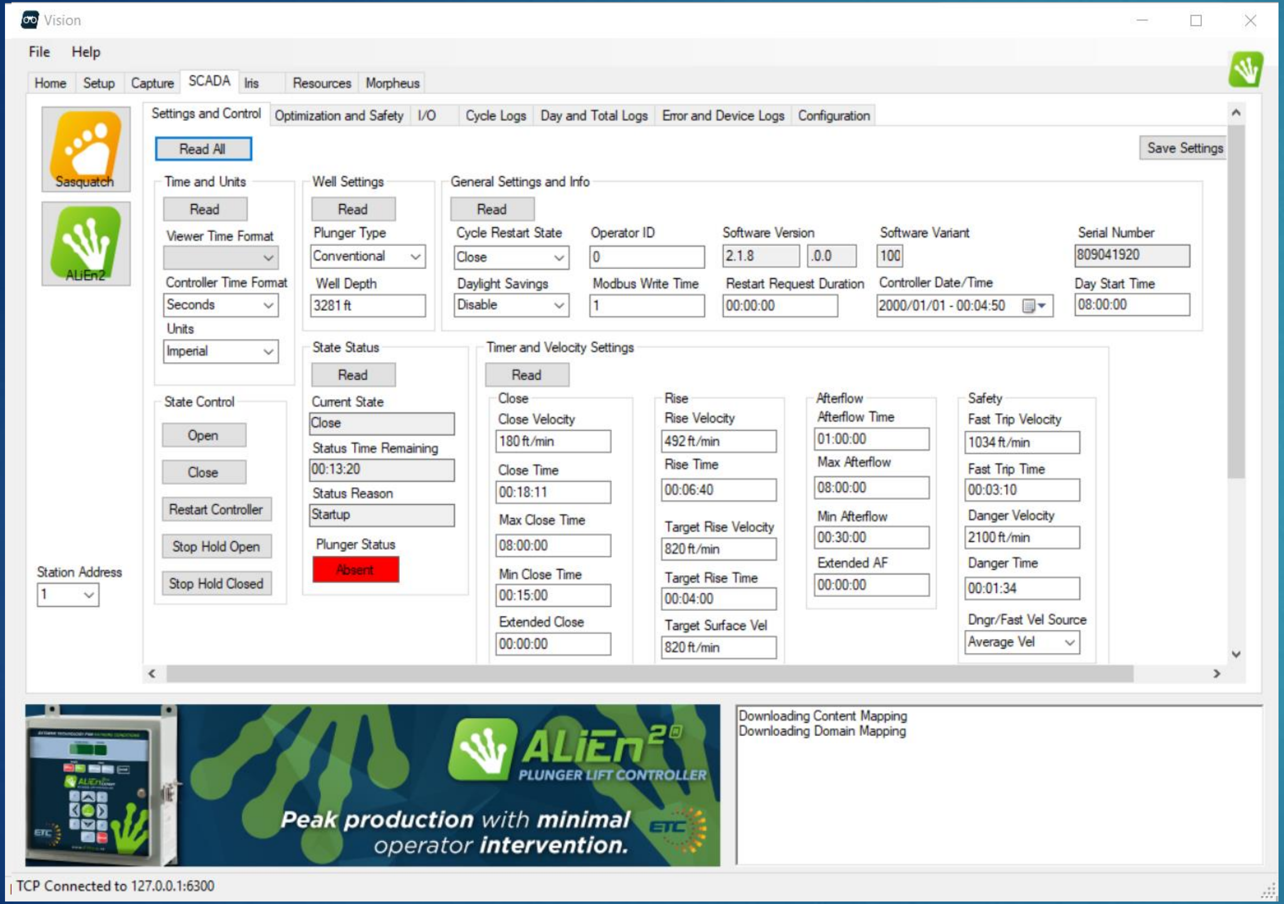
Peak production with minimal operator intervention.

TCP Connected to 127.0.0.1:6300



ETC
EXTREME TELEMATICS CORP.

Vision and ALiEn2 Simulator (TCP)



Time and Units
Viewer Time Format:
Controller Time Format: Seconds
Units: Imperial

Well Settings
Plunger Type: Conventional
Well Depth: 3281 ft

General Settings and Info
Cycle Restart State: Close
Operator ID: 0
Software Version: 2.1.8 .0.0
Software Variant: 100
Serial Number: 809041920
Daylight Savings: Disable
Modbus Write Time: 1
Restart Request Duration: 00:00:00
Controller Date/Time: 2000/01/01 - 00:04:50
Day Start Time: 08:00:00

State Control

Station Address: 1

State Status
Current State: Close
Status Time Remaining: 00:13:20
Status Reason: Startup
Plunger Status: Absent

Timer and Velocity Settings

Close
Close Velocity: 180 ft/min
Close Time: 00:18:11
Max Close Time: 08:00:00
Min Close Time: 00:15:00
Extended Close: 00:00:00

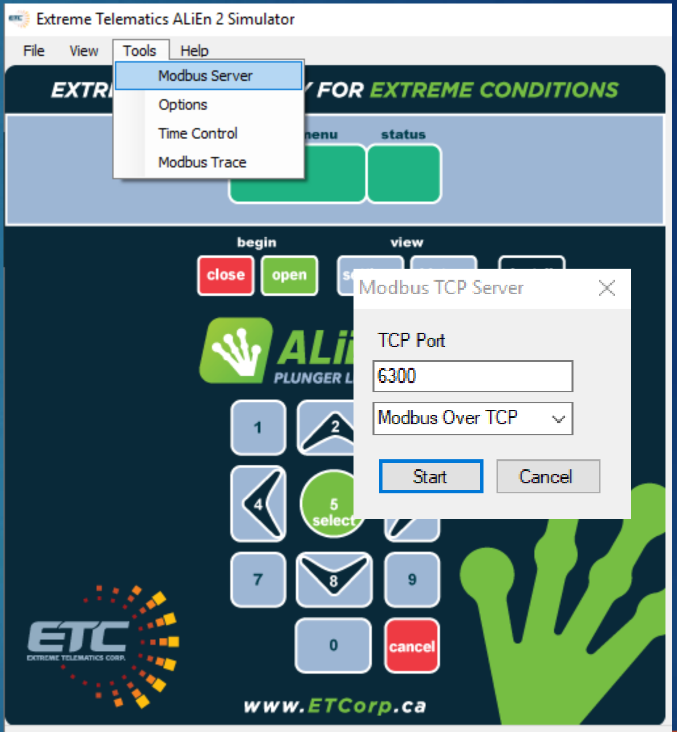
Rise
Rise Velocity: 492 ft/min
Rise Time: 00:06:40
Target Rise Velocity: 820 ft/min
Target Rise Time: 00:04:00
Target Surface Vel: 820 ft/min

Afterflow
Afterflow Time: 01:00:00
Max Afterflow: 08:00:00
Min Afterflow: 00:30:00
Extended AF: 00:00:00

Safety
Fast Trip Velocity: 1034 ft/min
Fast Trip Time: 00:03:10
Danger Velocity: 2100 ft/min
Danger Time: 00:01:34
Dngr/Fast Vel Source: Average Vel

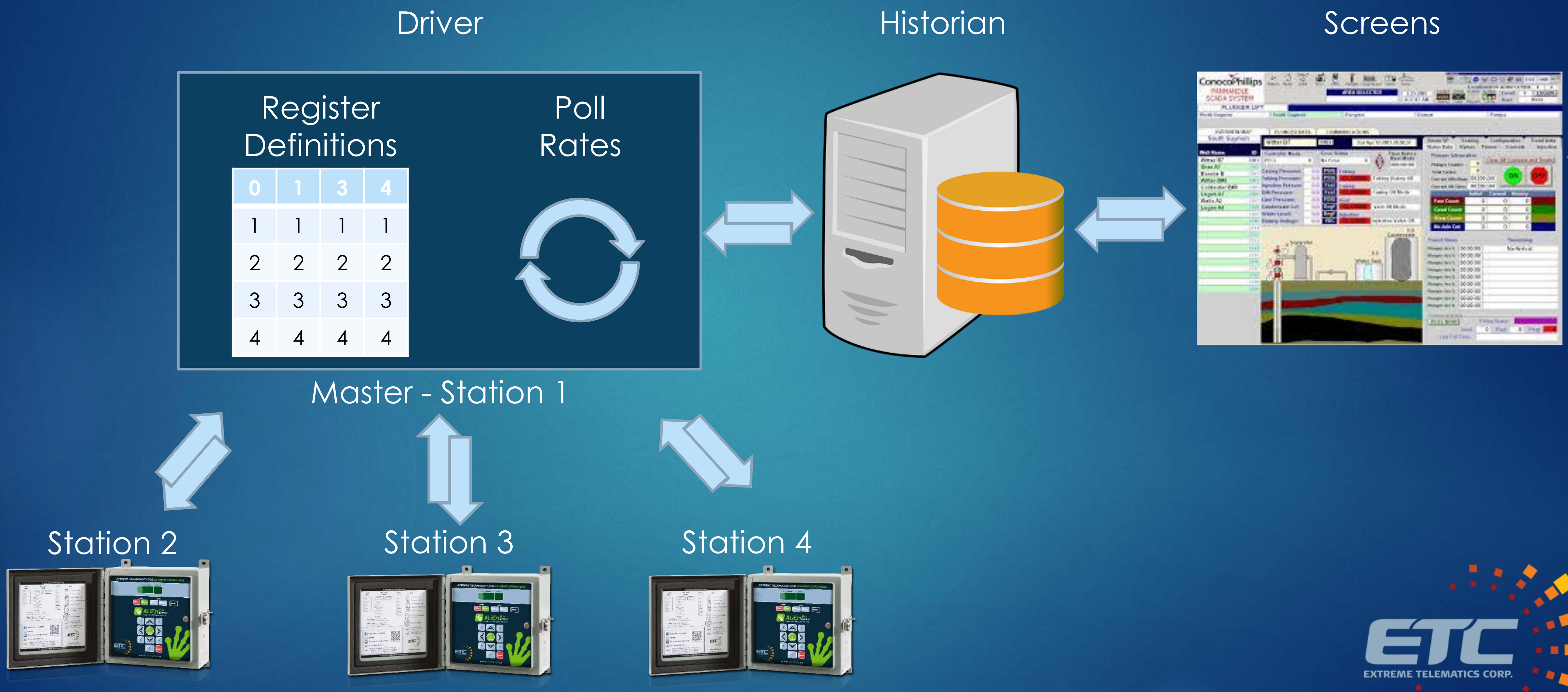
```
Downloading Content Mapping
Downloading Domain Mapping
```

TCP Connected to 127.0.0.1:6300

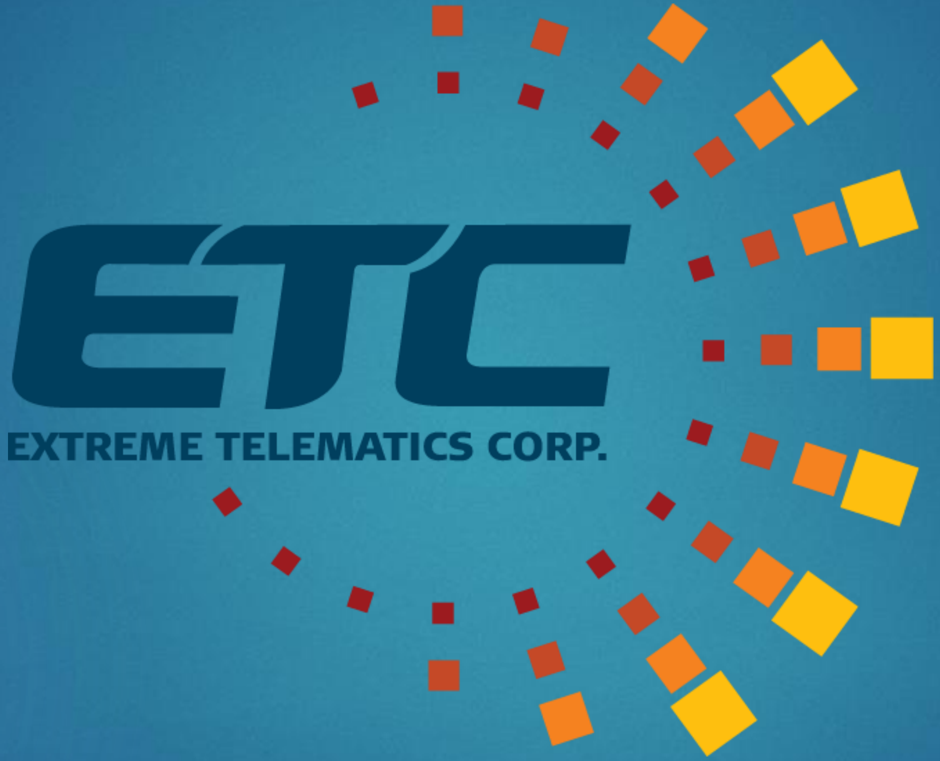


TCP Port: 6300
Modbus Over TCP

Field Deployment



0	1	3	4
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4


ETC
EXTREME TELEMATICS CORP.