RFC: 1977

ASSIGNMENT 2

DSLASER PROTOCOL
PROTOCOL SPECIFICATION

DSLASER Protocol Specification

This document specifies the DSLASER protocol utilized by the Death Star Super Laser system for communicating on an industrial control system (ICS) level network. It is traditional use is to communicate from the commander terminal to the server responsible for instructing the Super Laser to fire.

Servers and programmable linear controllers (PLC) on this network will only respond to requests made by the command terminal. Due to the internal and closed nature of this system, no encryption standard is utilized to encode traffic. All encoding of traffic is the UTF-8 standard.

Network Access

This system utilizes port 1977 for access because it is not currently used for any other commonly or officially recognized service. Normally, the network will be hosted on a private network between all clients and server(s). Additionally, since the communication must be expected to be reliable with recent traffic in the case of a loss of integrity, TCP is used.

Each connection is handled on a different thread which utilizes an ephemeral port assigned from the core handshake. This allows the server to handle as many connections as there are threads available on the server itself. Additionally, it prevents the need for the server to be reopened in the case of terminal connection failures.

Lastly, a terminal should only need to initiate a connection to the server if it will go through with the firing process.

Security Features

DSLASER has a special behavior to prevent exploitation by the Rebel Alliance. After being hosted, if one of the following occurs, it will cause a fatal error to be thrown and the client will be disconnected from the connection.

1. Repeated COUNTDOWN_INITIATE requests are sent
2. An incorrect COUNTDOWN_DECREMENT_REQUEST request is sent
3. Repeated FIRE_LASER_REQUEST requests are sent

Message Types

There are five types of messages in the DSLASER protocol onboard the Death Star. The messages are COUNTDOWN_INITIATE, COUNTDOWN_DECREMENT, FIRE_LASER, FIRE_LASER_CONFIRMATION, and COMMUNICATION_SHUTDOWN. Each of these messages has a request and a response format which are listed on the following pages.

Message Code	Message
0x01	COUNTDOWN_INITIATE
0x02	COUNTDOWN_DECREMENT
0x03	FIRE_LASER
0x04	FIRE_LASER_CONFIRMATION
0x05	COMMUNICATION_SHUTDOWN

Response Codes

There are three response types: 0x00, 0x01, and 0x2. Each one indicates the specific response to the message by a system on the network.

Response Code	Response
0x00	Operation was successful; no error
0x01	ERR: Invalid Operation
0x02	ERR: Malformed Message

COUNTDOWN_INITIATE (0x01)

This message is used to initiate the countdown on the DSLASER system. A message code and a response code will be present in both the request and the response. However, the response will additionally include an integer value that will represent the countdown value which can be a value in the range of 5 – 100.

COUNTDOWN_INITIATE (Request)

Response	Length of Bytes
Message Code	2
Response Code	2

COUNTDOWN_INITIATE (Response)

Response	Length of Bytes
Message Code	2
Response Code	2
Countdown	4

COUNTDOWN_DECREMENT (0x02)

This message is used to decrement the countdown on the DSLASER system after a countdown has been initiated. A message code and a response code will be present in both the request and the response. The request value will be the next expected integer value in the sequence approaching to, and including, 0. A response from the server will be issued which will then confirm the decrement request and declare the current value of the countdown.

COUNTDOWN_DECREMENT (Request)

Response	Length of Bytes
Message Code	2
Response Code	2
Countdown	4

COUNTDOWN_DECREMENT (Response)

Response	Length of Bytes
Message Code	2
Response Code	2
Countdown	4

FIRE_LASER (0x03)

This message is used to fire the super laser on the DSLASER system after the countdown on the server has reached 0. A message code and a response code will be present in both the request and the response. A response from the server will be issued which will feature the string ‘Fired’ to indicate that the server has begun the firing sequence.

FIRE_LASER (Request)

Response	Length of Bytes
Message Code	2
Response Code	2

FIRE_LASER (Response)

Response	Length of Bytes
Message Code	2
Response Code	2
Firing Notification	5

FIRE_LASER_CONFIRMATION (0x04)

This message is used to confirm the firing of the super laser on the DSLASER system. A message code and a response code will be present in both the request and the response. A response from the server will be issued which will feature a string of up to 40 bytes that will provide information relating to the post-firing analysis.

FIRE_LASER_CONFIRMATION (Request)

Response	Length of Bytes
Message Code	2
Response Code	2

FIRE_LASER_CONFIRMATION (Response)

Response	Length of Bytes
Message Code	2
Response Code	2
Firing Confirmation	40

COMMUNICATION_SHUTDOWN (0x05)

This message is used to shutdown communication between the server and the client on the DSLASER system. A message code and a response code will be present in both the request and the response.

COMMUNICATION_SHUTDOWN (Request)

Response	Length of Bytes
Message Code	2
Response Code	2

COMMUNICATION_SHUTDOWN (Response)

Response	Length of Bytes
Message Code	2
Response Code	2

Expected Behavior

In order for the DSLASER to properly instruct the death star to fire, the following is to take place:

1. A COUNTDOWN_INITIATE request is to be sent to the server by the client which will cause the generation of a countdown from 5-100 on the server
    a. A response is issued which will include the countdown's current count
2. A COUNTDOWN_DECREMENT request is to be sent to the server by the client of the next value up to and including 0
    a. A response will be issued by the server of the value sent
    b. This request-response cycle will continue until a response of 0 is received.
3. A FIRE_LASER request is to be sent to the server by the client
    a. A response will be issued by the server which will respond with the UTF-8 encoded text of 'Fired'
4. A FIRE_LASER_CONFIRMATION request is to be sent to the server by the client
    a. A response will be issued by the server which will respond with the UTF-8 encoded text of authentication text
5. A COMMUNICATION_SHUTDOWN request is to be sent to begin the shutdown procedure
    a. A response will be issued by the server which will indicate the shutdown has occurred.