IB-11B043

JUNE 2003

ATA CONTROLLER

PITS TARGET

INSTRUCTION BOOK

INDUSTRIAL INDEXING SYSTEMS, Inc.

Revision - 0
Approved By:

TABLE OF CONTENTS

1.0 PURPOSE

To describe ATA PITS Target control. The target protocol is designed to facilitate target commands described in this document.

ACRONYM LIST				
PITS			Portable Infantry Target System	
SES			Sound Effects Simulator	
CES			Combat Effects Simulator	
BES			Battle Effects Simulator	
NES			Night Effects Simulator	
MSD			Miles Shootback Device	
IMTM			Infantry Mobile Target Mover	
RFCM			Radio Freq. Control Module	
AIL			Armored Infantry Lifter	
SATL			Stationary Armored Target Lifter	
TK			Tank Kill	
PHI			Positive Hit Indicator	
MG			Machine Gun Fire	
GF			Gun Fire	

2.0 TARGET COMMANDS

TARGET COMMANDS		TARGET ADDRESS 1 TO 999		
COMMAND	**PARAMETERS**	**DEVICE**	**DESCRIPTION**	**QUESTIONS**
Set Target Up (Once per command)			Puts target up and restarts mode sequence. Resets # of hits.	
Set Target Down (Once per command)			Puts target down, terminates mode sequence and stops counting hits & kills	
Get Hits	# hits Max 255		Requests # of hits	
Get Kill Score	# kills Max 255		Requests score - # of kills	
Set Clear Score (Once per command)			Clears # Hits and # kills	
Set Mode				
	Auto		Target drops after kill and stays down; Target Up resets # hits	
	Up After Hit (Kill)		5 seconds after kill will come back up until #cycles then stays down; Target Up resets # hits	
	Up No Hit		Target goes up for 5 seconds, down for 3, until kill then it stays down; Target Up resets # hits	
	Hold		Does not move UP/Down but still counts hits & kills when up	
	Cycle		Up and down (mainly for testing) 10 cycles 3 sec separation and stays down	
Set Muzzle Flash (Once per command)		SES/NES	Qty 3 60ms pulses then stop for each command execution	
Set MoonGlow On/Off			Moonglow light is only lit while target is up.	
Set Positive Hit Indicator On/Off			When on this cause PHI to light for 1 second after hit.	
Set Miles Shootback Device On/Off		MSD	This causes MSD to turn on	Pulse or ON/OFF?
Set Tape On/Off		SES	Sound effects	Pulse or ON/OFF?
Set Sensitivity	1-9		Length of Hit pulse, longer with larger caliber weapon	
Set Hits to Kill	1-10		Determines how many hits will "kill" target, stop counting "Hits" when "Kill" reached except burst mode	
Set Number of cycles	1-255		#cycles for "Up after Hit (Kill)" mode	
Set Burst Mode On/Off			# Hits continues to count even when target is "Killed" until target reaches down position	

2.0 TARGET COMMANDS (cont'd)

TARGET COMMANDS		TARGET ADDRESS 1 TO 999		
COMMAND	PARAMETERS	DEVICE	DESCRIPTION	QUESTIONS
Get Battery status	0=Battery low, 1=OK		Battery voltage below 11 VDC = low	
Get Communication status	0=Timeout, 1=Bad Com		Timeout is no response from target, Bad comm is bad checksum	
Get Inputs	16 bits = 16 inputs		Miles detect one of input bits	
Get Hit Device	0=Hit Sw; 1=Miles2000		Hits coming from miles or hit switch?	Still don't have full Miles Spec?? Ouch!!
Get Motor Status	0=Stalled, 1=OK		Stalled detected by over current	
Set Goup Broadcast Address	1-999		Sets an address in controller that will respond to a broadcast message	
Broadcast	FFFFh		Universal broadcast message	

2.1 OPERATION CONSIDERATIONS

1) A Target will not change modes until Set Down or it's at the end of a mode cycle.

2) Miles Hit and Shoot back devices not fully implemented as of 5/29/03 due to lack of information.

3.0 PACKET PROTOCOL INTRODUCTION

Targets will act under three addressing modes:

1) Explicit: Host addresses one target and receives response from that one target.
2) Broadcast All: Host can send data to all targets at once, type 3 messages with address of FFFFh.
3) Broadcast Group: Host can send data to a group of targets; type 3 messages with group address.

Targets only respond when explicitly addressed. Targets do not respond to broadcast TYPE 3 messages.
Target explicit addresses are read from the address switches.

Targets will always act on a broadcast all TYPE 3 message with no response packet.

Targets group addressing is explicitly set with a TYPE 2 message. Once set the target will act on a TYPE 3 message with an address of its group setting and will not send a response packet.

Here in hexadecimal (hex for short) values will be followed by h, therefore a hexadecimal value of 0E will be denoted as 0Eh.

Here in "A" indicates an ASCII byte character A. The hex value for "A" is 41h.

4.0 DATA TYPE 0 PACKET

Packet type 0 is the normal data packet between host and target. The host and target send identical packet formats when using type 0 packets. The Host will send 20 bytes to the target, and the target will respond with 20 bytes back to the Host.

Byte	Section	Description	
0	Header	"A"	prefix char 1
1		"T"	prefix char 2
2		"X"	prefix char 3
3		type	type 0 = write / read
4		length	packet body length
5	Body	spare	
6		target addr	target addr A
7		target addr	target addr B
8		commands	bits 7 - 0, one shot commands
9		commands	bits 15 - 8, on / off commands
10		inputs	bits 7 - 0
11		inputs	bits 15 - 8
12		outputs	bits 7 - 0
13		outputs	bits 15 - 8
14		hits	number of hits 0 - 99
15		score	number of kills 0 - 99
16		cycles	number of cycles 1 - 99
17		settings	sensitivity: bits 7 - 4, hits to kill: bits 3 - 0
18		mode	mode: 0 - 5
19	Cksum	cksum	2's complement of the sum of bytes 3 - 18

The Host sends Operational data to the target in bit commands of bytes 8 and 9, also cycles, settings, and mode settings of bytes 16 thru 19 respectively.

The target will send its status information back to the host in the input, output, hits, and score bytes 10 thru 15. The target ignores the information sent by the host in these bytes.

4.1 LENGTH BYTE 4

For a TYPE 0 data packet, length is 14 (0Eh) for both target and Host.

4.2 MODE BYTE 18 SETTINGS

0 No mode selected (power up state)
1 Auto - target drops and stays down after kill
2 Auto - target up after kill
3 Auto - target up no hit
4 Hold - does not move up / down
5 Cycle - target goes up / down for 10 cycles (testing)

4.3 HOST COMMAND BYTE BIT FORMAT

The bits in byte 8 are intended to act like a momentary switch or one shot. In that the bit creates an event the target executes upon.

The bits in byte 9 the target response follows the bit.

Byte	Bit	Description	
8	0	SetTargetUp	on - Host sends once
	1	SetTargetDown	on - Host sends once
	2	SetClearScore	on - Host sends once
	3	SetMuzzleFlash	on - Host sends once
	4		
	5		
	6		
	7		

Byte	Bit	Description	
9	0	SetBurstMode	on / off
	1	SetPHI	on / off
	2	SetMoonGlow	on / off
	3	SetMilesShootbackDevice	on / off
	4	SetTape	on / off
	5		
	6		
	7		

4.4 TARGET INPUTS STATUS BITS FORMAT

Byte	Bit	Description	
10	0	MotorStatus	0 = stalled, 1 = OK
	1	TargetDownSwitch	0 = target not down, 1 = target down
	2	TargetUpSwitch	0 = target not up, 1 = target up
	3	Test	1 = test input off, 0 = test input on
	4	Spare 1	
	5	Spare 2	
	6	Spare 3	
	7	Miles input	

Byte	Bit	Description	
11	0	HitDevice	0 = hit switch, 1 = Miles Shootback
	1		
	2		
	3		
	4		
	5		
	6		
	7		

4.5 TARGET OUTPUTS STATUS BYTES BIT FORMAT

Byte	Bit	Description	
12	0	MuzzleFlash	ON/OFF
	1	MoonGlow	ON/OFF
	2	BattleEffectSimulator	ON/OFF
	3	HitIndicator	ON/OFF
	4	LowBattery	ON/OFF, follows state of power lamp
	5	Spare1	ON/OFF
	6	Spare2	ON/OFF
	7	Spare3	ON/OFF

Byte	Bit	Description	
13	0		
	1		
	2		
	3		
	4		
	5		
	6		
	7		

5.0 QUERY TYPE 1 PACKET

A query packet can be sent by the Host to retrieve data from a target without the target acting on any of the operational bytes in a typical 20byte TYPE 0 data packet.

Target ignores operational bytes from Host. The body length byte could be 3 without effecting target response.

Example Query to target with address 1:

Host Sends:

“A”,”T”,”X”,01h,03h,00h,00h,01h,FBh

OR

“A”,”T”,”X”,01h,0Eh,00h,00h,01h,00h,00h,00h,00h,00h,00h,00h,00h,00h,00h,00h,00h,F0h

Target Response when inputs and outputs are 0, hits and kills are 9 and 3 resp., cycles is 2, sensitivity and hits to kill are both 3, and mode is 1:

“A”,”T”,”X”,01h,0Eh,00h,00h,01h,00h,00h,00h,00h,00h,00h,09h,03h,02h,33h,01h,AEh

6.0 SET BROADCAST GROUP ADDRESS TYPE 2 PACKET

Allows the Host computer to set a targets' group broadcast address using a typical 20 byte packet with the targets broadcast group address in command bytes 8 and 9. Target will always respond with 20 bytes and the sent broadcast address in bytes 8 and 9.

Target ignores operational bytes from Host. The body length could be 5 from the Host without effecting target response or set operation against the sent broadcast address.

Example BC Group address of 100 set to target with explicit address 999:

Host Sends:

"A","T","X",02h,03h,00h,03h,E7h,00h,64h,ADh

OR

"A","T","X",02h,0Eh,00h,03h,E7h,00h,64h,00h,00h,00h,00h,00h,00h,00h,00h,00h,00h,A2h

Target Response when inputs and outputs are 0, hits and kills are 9 and 3 resp., cycles is 2, sensitivity and hits to kill are both 3, and mode is 1:

"A","T","X",02h,0Eh,00h,03h,E7h,00h,64h,00h,00h,00h,00h,09h,03h,02h,33h,01h,60h

7.0 GET TARGET SFO AND REVISION TYPE 4 PACKET

Allows the Host computer to get a targets' firmware number with revision. Target will always respond with 20 bytes with a ASCII string in bytes 8 thru 18 denoting the SFO (O is alphabetic ASCII 4Fh) number and revision.

NOTE

Industrial Indexing Systems internally archives firmware using SFO numbers with associated revisions. The First PITS Targets have been assigned SFO number 3455 as of 5/23/03.

Target ignores operational bytes from Host. The body length could be 3 from the Host without effecting target response.

Example gets to target with explicit address 10:

Host Sends:

"A","T","X",04h,03h,00h,00h,0Ah,EFh

OR

"A","T","X",04h,0Eh,00h,00h,0Ah,00h,00h,00h,00h,00h,00h,00h,00h,00h,00h,00h,E4h

Target Response when SFO # is 3455 at revision 1 ASCII string in bytes 8 thru 18 will be "SFO-3455R01":

"A","T","X",04h,0Eh,00h,00h,0Ah,53h,46h,4Fh,2Dh,33h,34h,35h,35h,52h,30h,31h,4Bh

APPENDIX A - FIRMWARE DOWNLOAD TO ATA TARGETS

A.0 INTRODUCTION

The ATA target control board has a download Kernel programmed in upper FLASH memory to facilitate RS485 network firmware download, specifically SFO-3455 as of 5/23/03. Other application firmware could be loaded into the target control board assuming certain guidelines required by the download Kernel are met.

The Download Kernel was written to accept Intel Hex Records, herein IHEX for short, over the RS485 network.

To invoke the download Kernel the firmware will accept a special packet that will cause a code jump to the Kernel. The Kernel at initial execution will ERASE all FLASH memory for target application code (SFO-3455 as an example). If power is cycled at this point the target control board will jump back to the download Kernel in that no application firmware exists, during power-up.

IMPORTANT NOTE

The Kernel will always send a NACK character 015h on any error in the IHEX format. It also assumes the Host will resend all records again in the event of an error. If a target NACKS again on the second attempt, the Host shall need to send the ERASE IHEX packet discussed later herein.

Herein a NACK character is the ASCII 15h byte.

Herein an ACK character is the ASCII 06h byte.

The download Kernel may be invoked to send an ACK on receipt of every record. ACKs may be elected to be turned off if a broadcasted firmware download is desired from the Host, however NAKs can never be turned off.

A.1 INTEL HEX RECORDS

The Intel HEX file is an ASCII text file with lines of text that follow the Intel HEX file format. Each line in an Intel HEX file contains one HEX record. These records are made up of hexadecimal numbers that represent machine language code and/or constant data. Intel HEX files are often used to transfer the program and data that would be stored in a ROM or EPROM. Most EPROM programmers or emulators can use Intel HEX files.

A.1.1 RECORD FORMAT

An Intel HEX file is composed of any number of HEX records. Each record is made up of five fields that are arranged in the following format:

:llaaaatt_dd..._cc

Each group of letters corresponds to a different field, and each letter represents a single hexadecimal digit. Each field is composed of at least two hexadecimal digits, which make up a byte as described below:

: is the colon that starts every Intel HEX record.
ll is the record-length field that represents the number of databytes in **dd** field**.**.
aaaa is the address field that represents the starting address for subsequent data in the record.
tt is the field that represents the HEX record type.
dd is a data field that represents one byte of data. A record may have multiple data bytes. The number of data bytes in the record must match the number specified by the **ll** field.
cc is the checksum field that represents the checksum of the record. The checksum is calculated by summing the values of all hexadecimal digit pairs in the record modulo 256 and taking the two's complement.

Intel Hex Defined types (**tt** field):

00 data record
01 end-of-file record
02 extended 8086-segment address record.
04 extended linear address record.

Industrial Indexing Systems Unique IHEX types (**tt** field):

80 set ack character off
82 set ack character on
84 send Kernel revision
90 erase code space FLASH memory

A.2 DOWNLOAD KERNEL INVOCATION PACKETS

To get a target to accept new firmware the download Kernel needs to be running. This is accomplished by sending one of the invocation packets shown below:

Broadcasted Kernel Invocation:

"A","T",">",03h,03h,00h,FFh,FFh,FCh

Explicit Kernel Invocation with ACKs:

"A","T",">",00h,03h,01h,xxh,xxh,csh

Explicit Kernel Invocation without ACKs:

"A","T",">",00h,03h,00h,xxh,xxh,csh

Where: **xxh** is to be filled in with the targets address
csh is the checksum same as in a TYPE 0 data packet.

If the Host invokes the Kernel using the broadcast invocation then all targets listing will Erase their firmware and accept IHEX records without sending a ACK for each accepted record.

The Host has the option to invoke the Kernel individually by explicitly addressing targets and then starting the firmware download.

During a broadcasted downloads to all targets running the kernel; all targets on a given network will listen simultaneously for the IHEX records. If any one target detects an error the Host shall receive on NACK character. Targets could all try to send NACKS simultaneously generating some indeterminate return to the Host. Therefore the Host most assumes any return is bad.

A.3 EXAMPLE IHEX RECORDS

A.3.1 DATA RECORD

:10246200464C5549442050524F46494C4500464C33

where:

10	is the number of data bytes in the record.
2462	is the address where the data are to be located in memory.
00	is the record type 00 (a data record).
46...64C	is the data.
33	is the checksum of the record.

A.3.2 END-OF-FILE (EOF) RECORD

:00000001FF

where:

00	is the number of data bytes in the record.
0000	is the address where the data are to be located in memory. The address in end-of-file records is meaningless and is ignored. An address of 0000h is typical.
01	is the record type 01 (an end-of-file record).
FF	is the checksum of the record and is calculated as 01h + NOT (00h + 00h + 00h + 01h).

A.3.3 SET ACK RESPONSE OFF

:0000008080

where:

00	is the number of data bytes in the record.
0000	is the address where the data are to be located in memory. The address in end-of-file records is meaningless and is ignored. An address of 0000h is typical.
80	is the record type 80 (set acks off).
80	is the checksum of the record and is calculated as 01h + NOT (00h + 00h + 00h + 01h).

A.3.4 SET ACK RESPONSE ON

:000000827E

where:

00	is the number of data bytes in the record.
0000	is the address where the data are to be located in memory. The address in end-of-file records is meaningless and is ignored. An address of 0000h is typical.
82	is the record type 80 (set acks on).
7E	is the checksum of the record and is calculated as 01h + NOT (00h + 00h + 00h + 01h).

A.3.5 SEND KERNEL REVISION

:000000847C

where:

00	is the number of data bytes in the record.
0000	is the address where the data are to be located in memory. The address in end-of-file records is meaningless and is ignored. An address of 0000h is typical.
84	is the record type 80 (send rev).
7C	is the checksum of the record and is calculated as 01h + NOT (00h + 00h + 00h + 01h).

Target response:

30	is the ASCII “0” character for revision zero

A.3.6 ERASE FIRMWARE

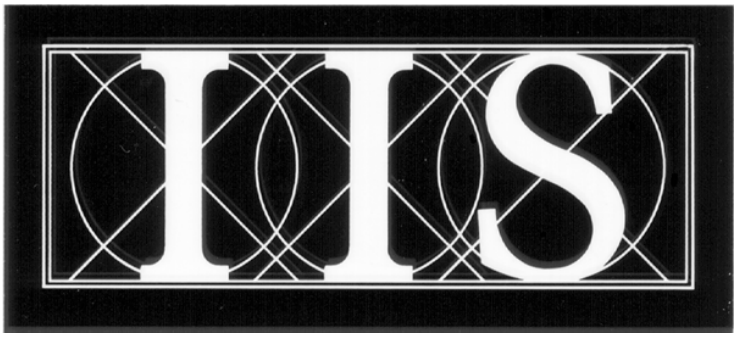
:0000009070

where:

00	is the number of data bytes in the record.
0000	is the address where the data are to be located in memory. The address in end-of-file records is meaningless and is ignored. An address of 0000h is typical.
90	is the record type 90 (erase).
70	is the checksum of the record and is calculated as 01h + NOT (00h + 00h + 00h + 01h).

An Erase operation can take 1 minute to accomplish before the target will respond to any other records. It’s advised that the Host poll the target with successive set ACK on records and wait for a return before sending new firmware.

IB-11B043



INDUSTRIAL INDEXING SYSTEMS INC.

626 FISHERS RUN
VICTOR, NEW YORK 14564

(585) 924-9181
FAX: (585) 924-2169

PRINTED IN USA