

TMEIC Photovoltaic Inverters Modbus Communication Interface Protocol For 1MW series

Rev. B

Model: PVL-L1000E, PVL-L1000E-H

TOSHIBA MITSUBISHI-ELECTRIC INDUSTRIAL SYSTEMS CORPORATION

© TOSHIBA MITSUBISHI-ELECTRIC INDUSTRIAL SYSTEMS Corporation, 2016 All Rights Reserved.



TABLE OF CONTENTS

1 Circui	it Configuration and Nomenclature	 	 		3
1.1	Abreviations				
1.2	Circuit Configuration	 	 		4
1.3	Operation States	 	 		5
2 Basic	Communication Specifications	 	 		6
2.1	Communication Procedure	 	 		6
2.2	System configuration	 	 		6
2.3	Precautions	 	 		7
3 <u>The o</u>	overview of Modbus TCP Communication protocol	 	 		8
3.1	Message Format	 	 		8
3.2	Supported Modbus Function Codes	 	 		8
3.3	Function Code Details	 	 		9
3.4	Register Data Format	 	 	1	1
4 Modk	bus/TCP Register Map	 	 	1	2
4.1	Register Map Structure	 	 	1	2
4.2	Input Registers (Fault data, Measurement)	 	 	1	3
4.3	Holding Registers (Command from monitoring system to the inverter)	 	 	2	22
5 Respo	onse Example				
5.1	Reading example for registers 30001~30056	 	 	2	24
5.2	Writing example for registers 40001~40010	 	 	3	30



1 Circuit Configuration and Nomenclature

This document describes the Modbus interface for TMEIC photovoltaic inverters. For installation and IP address setting, refer to the Installation Manual and IP address setting manual for communication unit.

1.1 Abreviations

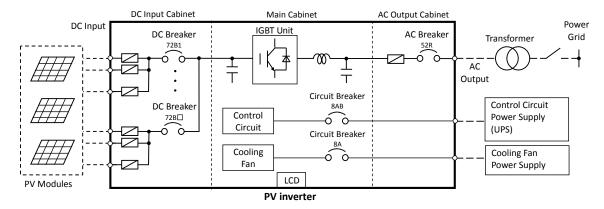
The following list contains the main abbreviations used throughout this text.

Name	Descriptions
52R	AC side circuit breaker
72B□	DC side circuit breaker
8AB, 8B	Control power supply miniature circuit breaker
8A	Fan power supply miniature circuit breaker
88F	Magnetic contactor for the cooling fan supply
ACB	Air Circuit Breaker
AVR	Automatic Voltage Regulator
ACR	Automatic Current Regulator
GFDI	Ground Fault Detection and Interruption
MC	Magnetic Contactor
MCCB	Molded Case Circuit Breaker
UPS	Uninterruptible Power Supply

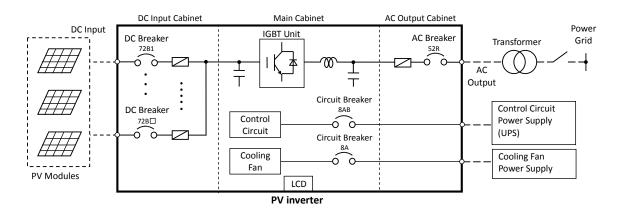


1.2 Circuit Configuration

The following figure shows as an example, the circuit configuration for the inverter. Different models may have different number of inputs and different circuit configuration. Refer to the Instruction Manuals and Schematic Diagrams of the plant for further details and descriptions.



(a) Outside fuse input type.



(b) Inside input fuse protection type



1.3 Operation States

Operation states of the inverter are described as follows:

Operating State		Description			
	Stop	Typical situation	- Before initial start up - After MAJOR FAULT occurred - After stop operation		
۵	·		Operation is completely stopped. Starting operation is required to move to "Stand by" mode. Detection of a MAJOR FAULT results in this state.		
STOP	Stand by	Typical - At night or sunset situation - After MINOR FAULT or GRID FAULT occurred* The inverter is connected to DC input power and waiting for sta condition establishment. AC output is not connected to the grid (5 opened) and the main inverter circuit is gate-blocked (GB), which mean inverter switching is stopped.			
	AC-AVR		Transient state from "Stand by" to "DC-AVR". The inverter starts generating AC voltage, but not connected to the grid.		
97	DC-AVR	Transient state from "AC-AVR" to "MPPT Control" mode. The inverter is connected to the grid.			
Connected to the grid. Power delivering operation. Energy from PV modules are core energy and delivered to the grid. DC input voltage is control Maximum Power Point Tracking (MPPT) control.		ered to the grid. DC input voltage is controlled based on			
	Grid-connected Stand by	Temporary state caused mostly by insufficient DC input power. The inverter stops switching, but is connected to the grid.			

^{* :} After a Synchronization Loss (Minor Fault) or Phase Jump (Grid Fault) the inverter will go into Grid-connected Stand-by mode and not to Stand-by mode.

When a fault is detected, the inverter will either stop its operation and / or show fault message on the LCD. The faults are categorized in four levels.

Fault level	Description		
ALARM	Faults which do not affect the operation of the inverter. The inverter will continue to deliver power to the grid.		
GRID FAULT	Faults caused by abnormal voltage or frequency of the power grid. The inverter will stop operation and disconnect from the grid. After the abnormal grid condition is cleared, the inverter will restart automatically.		
MINOR FAULT Faults which affect normal operation of the inverter caused by temporation and disconnect from grid. After the abnormal conditions are cleared, the inverter will reautomatically.			
MAJOR FAULT Faults caused by abnormal condition which may damage the inverter will stop operation and disconnect both from DC input circuit grid. On site operation and detailed check by service personnel are received the system.			



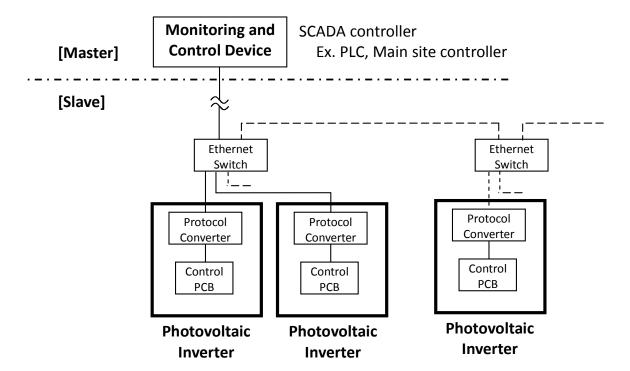
2 Basic Communication Specifications

2.1 Communication Procedure

The communication messages between the inverter and the external monitoring and control device are sent in Modbus TCP protocol data type. In the inverter, the protocol converter transmits prescribed commands to the control PCB in constant cycles and stores the response data to the inverter information area of the control PCB. This data is used as the response against the Modbus TCP request from external monitoring devices.

2.2 System configuration

The following figure shows an example of the communication system configuration. The inverter is regarded as Modbus slave and the monitoring and control device is regarded as Modbus master. One inverter can respond to a maximum of 3 sessions.



%Protocol Converter=UDS1100



2.3 Precautions

The Following precautions shall be considered when you configure communication system for monitoring and control.

- The preferred communication cycle is 1 second. However, please note that when the information is updated in the communication module, the previous data is overwritten. Therefore some information may be lost if the poling cycle is too long.
- Normal and reliable communication is not guaranteed Differences in communication cable length/location/route may cause disturbance and communication error.
- Surge protective device for communication line or other surge protection shall be installed when necessary. External surge voltage coming from communication line can be cause unexpected failure of the inverter.
- Monitoring and control device (Ex. SCADA system) shall be programed for error handling. Some recommended practices are; plural readings cut off communication by timeout, exclusion of invalid values by checking range of data values, etc.
- This communication function shall never be used for an application where safety of persons rely on.
- This communication function has delay time and shall not be used for the application which requires fast response This delay time is an indeterminate value which is composed from the internal processing delay and external transmission delay of the inverter. The data gotten from plural inverters at the same time are not synchronized.
- The inverter is not a measuring device. The measuring values returned from the inverter shall not be used for the purpose of electricity transaction and efficiency evaluation and other accuracy requested purposes.
- The inverter has no internal radio clock or GPS. The time stamp values of address 30001~3004 of the input register may not be accurate.
- Please use this document as a reference. This document is subjected to change without notice.



3 The overview of Modbus TCP Communication protocol

3.1 Message Format

Modbus/TCP



Unit Identifier is set to '1'

3.2 Supported Modbus Function Codes

Supported function codes are listed in the following table.

Code	Function Name	Description	
04 (0x04)	Read input registers	Reading input registers at once	
16 (0x10)	Write multiple registers	Writing a block of contiguous registers at once	



3.3 Function Code Details

1) Function code 04 (0x04) Read Input Registers

* Request

Byte offset	Description	Data
0	Function Code	0x04
1	Starting address Hi	0x0000 to 0xFFFF
2 Starting address Lo		
3	Quantity of registers Hi	1 to 125
4 Quantity of registers Lo		(0x0001 \sim 0x007D)

* Response

Response				
Byte offset	Description	Data		
0	Function Code	0x04		
1	Byte count	2 x N		
2	Register value 1 Hi			
3	Register value 1 Lo			
•••	Register value N Hi			
	Register value N Lo			

* Error

Byte offset	Description	Data
0	Error Code	0x84
1	Exception Code	See table below

* Error code list

Exception Code	Name	Description	
01	Illegal Function	The requested function code is other than 4 or 16	
02	Illegal Data Address	Starting address and starting address + quantity of registers is out of	
		Modbus/TCP register map (30001 \sim 30067)	
04	Slave Device Failure	Package received from inverter contains errors	
05	Acknowledge	Modbus/TCP unit is in initializing state (Communication task not	
		working)	
0A	Gateway Path Unavailable	Error in sending message from the Modbus/TCP unit to the inverter	
OB	Gateway Target Device Failed	Timeout in receiving message from inverter	
	to Respond		



2) Function code 16 (0x10) Write Multiple Registers

* Request

ricquest			
Byte offset	Description	Data	
0	Function Code	0x10	
1	Starting address Hi	0x0000 \sim 0xFFFF	
2	Starting address Lo		
3	Quantity of registers Hi	1 ~ 123	
4 Quantity of registers Lo		$(0x0001 \sim 0x007B)$	
5	Byte count	count 2 x N	
6	Register value 1 Hi		
7	Register value 1 Lo		
	Register value N Hi		
•••	Register value N Lo		

* Response

Byte offset	Description	Data
0	Function Code	0x10
1	Starting address Hi	0x0000 \sim 0xFFFF
2 Starting address Lo		
3 Quantity of registers Hi		1 ~ 123
4 Quantity of registers Lo		(0x0001 \sim 0x007B)

* Error

Byte offset	Description	Data
0	Error Code	0x90
1	Exception Code	See table below

* Error code list

Exception Code	Name	Description	
01	Illegal Function	The requested function code is other than 4 or 16	
02	Illegal Data Address	Starting address is other than 40001 = physical address 0, or	
		quantity of registers different than 12	
03	Illegal Data Value	Package received from inverter contains errors	
0A	Gateway Path Unavailable	Error in sending message from the Modbus/TCP unit to the	
		inverter	
OB	Gateway Target Device Failed	Timeout in receiving message from inverter	
	to Respond		



3.4 Register Data Format

4 types of data format are supported

Format	Description		
INT16	Signed 2 bytes integer		
UINT16	Unsigned 2 bytes integer		
INT32	Signed 4 bytes integer		
UINT32	Unsigned 4 bytes integer		

1) INT16

Signed 2 byte integer.

From -32768 ~ 32767.

Big endian

H L

2) UINT16

Unsigned 2 byte integer.

From 0 ~ 65535.

Big endian

н	L
---	---

3) INT32

Signed 4 byte integer.

From -2147483648 ~ 2147483647.

Big endian

HW	ORD	LW	/ORD
Н	L	Н	L

4) UINT32

Unsigned 4 byte integer.

From 0 ~ 4294967295.

Big endian

нw	ORD	L WORD		
Н	L	Н	L	



4 Modbus/TCP Register Map

4.1 Register Map Structure

Input registers (Read only)

Register Address	Description
30001	Fault data and measurement from PV system (cyclic data)
30056	
30057	(Not Supported)

Holding registers (Write only)

	• •
Register Address	Description
30001	Commands from the monitoring system to the inverter
30067	
40011	(Not Supported)



4.2 Input Registers (Fault data, Measurement)

Operation status and measured data of PV system.

* This data is updated every 1 second.

Register Address	Description	Format	Range/Unit	Notes
30001	Data status	INT16	(0-1)	0:unknown*
				1:ACK
				*:unknown indicates an error in the
				control power supply of the inverter
				or a communication error between
				the inverter and communication
				converter.
30002	Time stamp (YYMMDD)	INT32	(0-991231)	The control board does not have a
30004	Time stamp (hhmmss)	INT32	(0-235959)	clock. It uses the clock of the LCD
				display.
				The value contained in these
				registers will be '770707070707' in
				the following conditions: 1) Soon after turning on the
				control power (while the LCD is
				starting).
				2) When the communication
				between the LCD and the
				control board is damaged
				3)
				Note: the time stamp may not be
				accurate
30006	(Reserved)	UINT32		
30008	Alarm flag	UINT16		Information coded as bit data
				D15-D8: Reserved
				D07-D05: Reserved
				D04: Reserved
				D03: Minor Fault
				D02: Alarm
				D01: Grid Fault
				D00: Major Fault
30009	Status bit 1	UINT32		0:recovered, 1:triggered See Status bit 1 table
30011	Status bit 3 Word-0	UINT32		See Status bit 1 table
30013	Status bit 3 Word-1	UINT32		See Status bit 3 table
30015	Status bit 3 Word-2	UINT32		See Status bit 3 table
30017	Status bit 3 Word-3	UINT32		See Status bit 3 table
30019	Status bit 3 Word-4	UINT32		See Status bit 3 table
30021	Status bit 3 Word-5	UINT32		See Status bit 3 table
30023	Status bit 3 Word-6	UINT32		See Status bit 3 table
30025	Status bit 3 Word-7	UINT32		See Status bit 3 table
30027	Energy	INT32	1kWh	1 kWh per unit
				9999999kWh is the maximum
				value. When the energy data reach
				100GW, going back to zero.
				99999999kWh +1kWh = 0kWh
				[Example]
				9999999kWh → 99999999
				This energy values are only stored
				every 15 minutes. Other data loss
				when power supply is down.
				Other energy measurement device required if you need accurate energy
				monitoring.
]		monitoring.



Register Address	Description	Format	Range/Unit	Notes
30029	(Reserved)	INT32	nange/ onic	110103
30023	Active power P	INT16	0.1kW	0.1kW per unit
30031	netive power i	111110	O.IKW	0.1kW per anic
				Note: Extremely small value is
				omitted to zero. (Ex. less than 1.5% of
				rated power. There may be cases
				where that differs among models or
				manufacturing date.)
30032	Reactive power Q	INT16	0.1kVAr	0.1kVAr per unit
				·
				A lagging reactive power is defined as
				a reactive power that increases the
				grid voltage and is displayed as a
				positive value.
				A Leading reactive power is defined
				as a reactive power that decreases
				the grid voltage and is displayed as a
				negative value.
				Note: Extremely small value is
				omitted to zero. (Ex. less than 1.5% of
				rated power. There may be cases
				where that differs among models or
30033	Power factor	INT16	(1.00=100)	manufacturing date.) 0.01 per unit
30033	rowel lactor	INTIO	(1.00-100)	0.01 per drift
				Lagging is defined as a power factor
				that increases the grid voltage and is
				displayed as a positive value.
				Leading is defined as a power factor
				that decreases the grid voltage and is
				displayed as a negative value.
				Note1: Negative and positive do not
				represent a power flow direction. A
				unity power factor can be set either
				as 100 or -100.
				Nata 2: Estado de la constitución de
				Note2: Extremely small value is omitted to zero. (Ex. less than 1.5% of
				· •
				rated power. There may be cases where that differs among models or
				manufacturing date.)
30034	Grid frequency	INT16	0.1Hz	50.0Hz → 500
3000.				60.0Hz → 600
30035	Grid voltage UV	INT16	0.1V	Vuv
30036	Grid voltage VW	INT16	0.1V	Vvw
30037	Grid voltage WU	INT16	0.1V	Vmu
30038	Inverter output current U	INT16	0.1A	lu
30039	Inverter output current V	INT16	0.1A	Iv
30040	Inverter output current W	INT16	0.1A	Iw
30041	DC input power	INT16	0.1kW	Pdc
30042	DC input voltage	INT16	0.1V	Vdc
30043	DC input current	INT16	0.1A	Idc
30044	Potential to ground PE	INT16	0.1V	Vpe
30045	Potential to ground EN	INT16	0.1V	Ven
30046 30047	(Reserved) Rev.current1	INT16	0.1A	+
30047	Rev.current1	INT16 INT16	0.1A 0.1A	
30048	(Reserved)	INT32	U.IA	+
30043	(neserveu)	111132		



Register Address	Description	Format	Range/Unit	Notes
30051	(Reserved)	INT16		
30052	(Reserved)	INT16		
30053	(Reserved)	INT32		
30055	(Reserved)	INT32		

 $^{^{\}star}$ The 'reserved' address shall be undecided address. These addresses are not always zero.



Status bit 1:

Bit	Name	Comments
Position		
D31		
D30		
D29		
D28		
D27		
D26	(Reserved)	
D25	(Reserved)	
D24	(Reserved)	
D23		
D22	(Reserved)	
D21	(Reserved)	
D20	(Reserved)	
D19	(Reserved)	
D18	(Reserved)	
D17	Remote Operation (0=Disable, 1=Enable)	Remote operation enabled/disabled status. Remote operation can be enabled through the LCD, I/O signal or through communications via Function Code 16 (0x10) address 40001. Local operation status is not included, thus there is no distinction between "Remote Only" and "Remote & Local"
D16	Run command status (0=Stop, 1=Start)	,
D15	External I/O Input 4 status (0/1=Open/Close)	
D14	External I/O Input 3 status (0/1=Open/Close)	
D13	External I/O Input 2 status (0/1=Open/Close)	
D12	External I/O Input 1 status (0/1=Open/Close)	
D11	72B Status (0=OFF, 1=ON)	72B1, 72B2,72B□status. This bit will turn 1 Whenever one of the breakers is in the ON position.
D10	(Reserved)	
D9	52R Status (0=OFF, 1=ON)	
D8	Inverter Status (0=GB, 1=DEB)	GB: Gate signal of the inverter is blocked. DEB: Gate signal of the inverter is de-blocked.
D7		
D6		
D5	(Reserved)	
D4	Grid-Connected Stand-By Mode	
D3	MPPT Mode	
D2	DC-AVR Mode	
D1	Stop Mode	Inverter GB and 52R OFF. Please use D16 to discern between inverter shutdown and inverter stopped due to a fault
D0	(Reserved)	
		•

^{*}The 'reserved' address shall be undecided address. These addresses are not always zero.



Status bit 3:

Position Position No. Code	Word	Bit	Item	Display	Details	Туре	Comments
O					Details	Туре	Comments
D				Couc			
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
O							
D							
O							
O							
O							
0 D5 298 0 D4 298 0 D3 82 UF306 Control power supply undervoltage Major fault 0 D2 298 Section of circuit error (CLK) Major fault 0 D0 78 UF303 Control circuit error (WDT) Major fault 1 D31 0 Omage: Control circuit error (WDT) Major fault 1 D30 0 Omage: Control circuit error (WDT) Major fault 1 D30 0 Omage: Control circuit error (WDT) Major fault 1 D29 0 Omage: Control circuit error (WDT) Major fault 1 D28 0 Omage: Control circuit error (WDT) Major fault 1 D28 0 Omage: Control circuit error (WDT) Major fault 1 D28 0 Omage: Control circuit error (WDT) Major fault 1 D25 0 Omage: Control circuit error (WDT) Omage: Control circuit error (WDT) Omage: Control circuit error (WDT) 1							
0 D4 298 UF306 Control power supply undervoltage Major fault 0 D2 298 Begin to the process of th							
D							
0 D2 298 0 D1 80 UF305 Control circuit error (CLK) Major fault 0 D0 78 UF303 Control circuit error (WDT) Major fault 1 D31 0 Image: Control circuit error (WDT) Major fault 1 D30 0 Image: Control circuit error (WDT) Major fault 1 D29 0 Image: Control circuit error (WDT) Major fault 1 D29 0 Image: Control circuit error (WDT) Image: Control circuit error (WDT) 1 D28 0 Image: Control circuit error (WDT)							
0 D1 80 UF305 Control circuit error (CLK) Major fault 0 D0 78 UF303 Control circuit error (WDT) Major fault 1 D31 0 Image: Control circuit error (WDT) Major fault 1 D30 0 Image: Control circuit error (WDT) Major fault 1 D30 0 Image: Control circuit error (WDT) Major fault 1 D28 0 Image: Control circuit error (WDT) Image: Control circuit error (WDT) 1 D28 0 Image: Control circuit error (WDT) Image: Control circuit error (WDT) 1 D28 0 Image: Control circuit error (WDT) Image: Control circuit error (WDT) 1 D26 0 Image: Control circuit error (WDT) Image: Control circuit error (WDT) 1 D24 0 Image: Control circuit error (WDT) Image: Control circuit error (WDT) 1 D24 0 Image: Control circuit error (WDT) Image: Control circuit error (WDT) 1 D25 0 Image: Control circuit error (WDT)				UF306	Control power supply undervoltage	Major fault	
0 D0 78 UF303 Control circuit error (WDT) Major fault 1 D31 0 </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
1 D31 0 1 D30 0 1 D29 0 1 D28 0 1 D27 0 1 D26 0 1 D25 0 1 D24 0 1 D23 0 1 D22 0 1 D21 0 1 D20 0 1 D19 0 1 D18 0 1 D16 108 UF810 DC current backflow 1(CSG1) Major fault Depends on circuit configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault	0	D1					
1 D30 0 1 D29 0 1 D28 0 1 D27 0 1 D26 0 1 D25 0 1 D24 0 1 D23 0 1 D23 0 1 D21 0 1 D20 0 1 D19 0 1 D18 0 1 D16 108 UF810 DC current backflow 1(CSG1) Major fault Depends on circuit configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault	0	D0	78	UF303	Control circuit error (WDT)	Major fault	
1 D29 0 1 D28 0 1 D27 0 1 D26 0 1 D25 0 1 D24 0 1 D23 0 1 D22 0 1 D20 0 1 D19 0 1 D18 0 1 D17 0 1 D16 108 UF810 DC current backflow 1(CSG1) Major fault Major fault Obepends on circuit configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault	1						
1 D28 0	1	D30	0				
1 D27 0 1 D26 0 1 D25 0 1 D24 0 1 D23 0 1 D22 0 1 D21 0 1 D20 0 1 D19 0 1 D18 0 1 D17 0 1 D16 108 UF810 DC current backflow 1(CSG1) Major fault Depends on circuit configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault	1	D29					
1 D26 0	1						
1 D25 0	1	D27	0				
1 D24 0	1						
1 D23 0	1	D25					
1 D22 0	1	D24	0				
1 D21 0 1 D20 0 1 D19 0 1 D18 0 1 D17 0 1 D16 108 UF810 DC current backflow 1(CSG1) Major fault configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault	1	D23	0				
1 D20 0	1	D22	0				
1 D20 0 1 D19 0 1 D18 0 1 D17 0 1 D16 108 UF810 DC current backflow 1(CSG1) Major fault configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault			0				
1 D19 0			0				
1 D18 0							
1 D17 0 D16 D18 UF810 DC current backflow 1(CSG1) Major fault Depends on circuit configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault							
1 D16 108 UF810 DC current backflow 1(CSG1) Major fault Depends on circuit configuration Used for the inverter with "DC negative grounding kit" 1 D15 48 UF114 DC current balance abnormal Major fault							
			108	UF810	DC current backflow 1(CSG1)	Major fault	configuration Used for the inverter with "DC negative grounding
	1	D15	48	UF114	DC current balance abnormal	Major fault	
							Reserved



						Rev A
Word	Bit	Item	Display	Details	Туре	Comments
Position	Position	No.	Code			
1	D13	170	UF230	Zero phase OC	Major fault	
1	D12	56	UF002	Inverter overcurrent 2	Major fault	
1	D11	64	UF107	DC overcurrent 3	Major fault	
1	D10	62	UF106	DC overcurrent 2	Major fault	
1	D9	60	UF108	DC overcurrent 1	Major fault	
1	D8	0			,	Reserved
1	D7	66	UF110	Zero phase overcurrent	Major fault	
1	D6	88	UF333	IGBT gate fault phase W	Major fault	
1	D5	86	UF332	IGBT gate fault phase V	Major fault	
1	D4	84	UF331	IGBT gate fault phase U	Major fault	
1	D3	74	UF301	Control circuit error (AD)	Major fault	
1	D2	72	UF128	Control power abnormal	Major fault	
1	D1	68	UF112	DC circuit abnormal	Major fault	
1	D0	58	UF101	DC overvoltage	Major fault	
2	D31	0	01101	DC Over voicage	iviajoi iault	
2						
	D30	0				
2	D29	0				
2	D28	0			1	
2	D27	0				
2	D26	0				
2	D25	0				
2	D24	0				
2	D23	0				
2	D22	0				
2	D21	0				
2	D20	0				
2	D19	0				
2	D18	0				
2	D17	70	UF120	DC ground fault (HCT)	Major fault	Depends on circuit configuration Used for the inverter with "DC Negative grounding kit"
2	D16	76	UF302	Control circuit error (FPGA)	Major fault	
2	D15	256	UF300	Flash memory error	Major fault	
2	D14	230	0.300	Tradit memory error	iviajor raure	
2	D13					
2	D13					
2	D11					
2	D11					
2	D10					
2	D9				+	
					+	
2	D7	0				Pacaryod
2	D6	0	11534.4	Cooling for the arrest	Nation for the	Reserved
2	D5	124	UF214	Cooling fan abnormal	Major fault	
2	D4	96	UF820	Repeated fault	Major fault	
2	D3	94	UF819	Repeated fault	Major fault	
2	D2	52	UF001	Inverter abnormal	Major fault	
2	D1	92	UF818	External trip	Major fault	Depending on I/O signal
2	D0	50	UF817	Emergency stop activated	Major fault	
3	D31					
3	D30					
3	D29					
3	D28					
3	D27					
	D26					
3	D20					
3	D25					



					1	Rev A
Word	Bit	Item	Display	Details	Туре	Comments
Position	Position	No.	Code			
3	D23					
3	D22					
3	D21					
3	D20					
3	D19					
3	D18					
3	D17					
3	D16					
3	D15					
3	D14					
3	D13					
3	D12					
3	D11					
3	D10					
3	D9					
3	D8					
3	D7					
3	D6					
3	D5	106	UF115	DC unbalance 1	Minor fault	
3	D4	98	UF307	Control power supply abnormal (AC-OV)	Minor fault	
3	D3	132	UF308	Control power supply abnormal (AC-UV)	Minor fault	
3	D2	130	UF823	8A open	Minor fault	
3	D1	164	UF103	DC undervoltage	Minor fault	
3	D0					
4	D31					
4	D30					
4	D29					
4	D28	22	UF892	External grid fault	Grid fault	Used by OVGR or other
						external relay signal
4	D27					
4	D26					
4	D25	18	UF207	Synchronization loss	Minor fault	
4	D24	16	UF221	Voltage phase jump	Grid fault	
4	D23	20	UF802	Open phase	Minor fault	
4	D22	14	UF803	Phase rotation error	Minor fault	
4	D21	12	UF220	Underfrequency	Grid fault	
4	D20	10	UF219	Overfrequency	Grid fault	
4	D19	8	UF218	Short time AC undervoltage	Minor fault	
4	D18	4	UF202	Grid undervoltage(UV)	Grid fault	
4	D17	6	UF217	Short time AC overvoltage	Minor fault	
4	D16	2	UF201	Grid overvoltage(OV)	Grid fault	
4	D15	254	UF832	Communication command time out	Minor fault	
4	D14					
4	D13					
4	D12					
4	D11					
4	D10					
4	D9					
4	D8	128	UF891	External minor fault	Minor fault	Depending on I/O
4	D7	126	UF213	Over temperature	Minor fault	
4	D6	178	UF053	52R OFF failure	Major fault	
4	D5	160	UF052	52R ON failure	Minor fault	
4	D4	172	UF253	AC voltage sensor error	Minor fault	
4	D3					
4	D2	122	UF206	Ctrl. Circuit error	Minor fault	
4	D1	120	UF807	Inverter overcurrent	Minor fault	
4	D0	54	UF003	Inverter OC.	Minor fault	
5	D31					
			·		*	



VA/a nal	D:4	lka sa	Diamlari	Dataila	T	Comments
Word Position	Bit Position	Item No.	Display Code	Details	Туре	Comments
5	D30	NO.	Code			
5	D30 D29					
5	D29					
5	D28					
5	D26					
5	D25					
5	D24					
5	D23					
5	D22					
5	D21					
5	D20					
5	D19					
5	D18					
5	D17					
5	D16					
5	D15					
5	D14					
5	D13					
5	D12					
5	D11					
5	D10					
5	D9					
5	D8					
5	D7					
5	D6					
5	D5					
5	D4					
5	D3					
5	D2					
5	D1					
5	D0					
6	D31					
6	D31					
6	D30					
6						
	D28					
6	D27					
6	D26					
6	D25					
6	D24					
6	D23					
6	D22					
6	D21					
6	D20					
6	D19					
6	D18					
6	D17					
6	D16					
6	D15					
6	D14					
6	D13					
6	D12					
6	D11					
6	D10	182	UA157	AMBIENT OT.	Alarm	
6	D9	180	UA825	52R not charged	Alarm	May be disabled
	55	100	07.023	5		depending on settings
6	D8	174	UA808	Grid voltage rise	Alarm	May be disabled
	50	1,7	0,1000			depending on settings
6	D7	176	UA211	SPD error	Alarm	acpenants on settings
U	U/	1/0	UAZII	21 12 (110)	Alai III	<u> </u>



NA/o nal	D:4	lk a sa	Disaless	Deteile	T a	Community
Word	Bit Position	Item	Display	Details	Туре	Comments
Position 6	D6	No. 168	Code UA159	DC ground fault(Voltage divider)	Alarm	Depends on circuit
0	D0	100	UA159	DC ground raun(voitage divider)	Aldilli	configuration
						Use for DC floating
						ground system
6	D5	166	UA119	DC ground fault(HCT)	Alarm	Depends on circuit
		100	UAIIS	De ground radit(rier)	Alaim	configuration
6	D4	158	UA890	External alarm	Alarm	Reserved
6	D3	162	UA102	DC-C Abnormal	Alarm	Reserved
6	D2	154	UA824	72B open	Alarm	DC breakers 72B1,
	52	131	071021	725 Spen	71101111	72B2,72B□is open
						status. (both/all open)
6	D1	150	UA804	Operation prohibition	Alarm	Startup is interlock
						status. (CNV SW ON. 52R
						locked. For maintenance
6	D0					and testing)
7	D31					
7	D30					
7	D29					
7	D28					
7	D27					
7	D26					
7	D25					
7	D24					
7	D23					
7	D22					
7	D21					
7	D20					
7	D19					
7	D18					
7	D17					
7	D16					
7	D15					
7	D14					
7	D13					
7	D12					
7	D11					
7	D10					
7	D9					
7	D8					
7	D7					
7	D6					
7	D5					
7	D4					
7	D3					
7	D2					
7	D1					
7	D0					

^{*}The 'reserved' address shall be undecided address. These addresses are not always zero.



4.3 Holding Registers (Command from monitoring system to the inverter)

Register address	Name	Format	Range/unit	Description
40001	Operation (OP2)	INT16	(0-3)	= '0': Used for setting time stamp in registers 40006 to 40010. Start/Stop command is not changed Setting of [P limit enable/disable] ~ [Reactive power Q command or power factor command] can not be done. = '1' Stop command: Goes to Stop mode when the inverter is in Start mode. If the inverter is in Stop mode, it keeps the Stop mode status. Settings for [P limit enable/disable] ~ [Reactive power Q command or power factor command] can be done. = '2' Start command: Goes to Start mode when the inverter is in Stop mode. If the inverter is in Start mode, it keeps the Start mode status. Note: There may be other conditions to clear before the inverter effectively starts. Settings for [P limit enable/disable] ~ [Reactive power Q command or power factor command] can be done. = '3' P limit, Q command or reactive power command: Start/Stop command is not changed Settings for [P limit enable/disable] ~ [Reactive power Q command or power factor command] can be done. For any value in register 40001, [Time stamp enable/disable][Time stamp] settings can be performed.
40002	P limit enable/disable	INT16	(0-1)	Enable/disable settings for active power P limit. The inverter output power will follow the MPPT when P limit is disabled. = '0' P limit disable = '1' P limit enable
40003	Active power P limit	INT16	0.1kW (0-)	0.1kW per unit 【Example】 250.0kW→2500 500.0kW→5000 1000.0kW→10000 【Restriction】 The active power may be limited to a lower value depending on the inverter maximum apparent power and the current irradiance (among other parameters).



Pogistor	Nama	Format	Pango /unit	Description Nev A
Register address	Name	Format	Range/unit	Description
40004	Q command enable/disable	INT16	(0-2)	Enable/disable settings for reactive power Q command
	or	20	(0 =)	and power factor command
	Power factor command			
	enable/disable			= '0' Q command disable, PF command disable
				Xinverter should run at power factor 1
				= '1' Q command enable, PF command disable
				= '2' Q command disable, PF command enable
40005	Reactive power Q command	INT16	(0-)	Reactive power Q (0.1kVAr per unit):
	or			A lagging reactive power is defined as a reactive power
	Power factor command			that increases the grid voltage and is displayed as a
				positive value.
				A Leading reactive power is defined as a reactive power
				that decreases the grid voltage and is displayed as a
				negative value.
				[[] [] [] [] [] [] [] [] [] [
				【Example】 +131.6kvar→ +1316
				+131.6kvar→+1316 -131.6kvar→-1316
				+263.3kvar →+2633
				-263.3kvar→-2633
				Power factor command (0.01 per unit):
				Lagging is defined as a power factor that increases the
				grid voltage and is displayed as a positive value.
				Leading is defined as a power factor that decreases the
				grid voltage and is displayed as a negative value.
				Note: Negative and positive do not represent a power
				flow direction. A unity power factor can be set either as 100 or -100
				100 01 -100
				【Example】
				+1.00:+100
				-1.00 : -100
				+0.95:+95
				-0.95 : -95
				[Restriction]
				The following two items will take priority over both
				reactive power Q command and power factor command
				(A) Power forton way (0.05), 4.00 ft 1, 11, 11
				1) Power factor range (0.85 to 1.00 for both leading
				and lagging power factors).
				2) Maximum apparent power of the inverter.
				Therefore, it may occur that the reactive power
				command and the power factor command are not
				followed in order to keep the system within the limits
				established in 1) and 2).
40006	Time Stamp Enable/Disable	INT16	(0-1)	= '0' Time Stamp Disabled
				= '1' Time Stamp Enabled
				Time stamp value for the inverter is set in
				registers 40007∼40010.
40007	Time Stamp (YYMMDD)	INT32	(0-991231)	YYMMDD
40009	Time Stamp (hhmmss)	INT32	(0-235900)	Hhmm00 (seconds are fixed and set to 00)

^{*} This is a write only data. All data should be written at once, starting from the starting address (40001)

^{*} Data out of range is discarded



5 Response Example

- Reading example for registers 30001~30056 5.1
- a-1) From Monitoring PC to inverter. Request while inverter is running

```
10 2012-05-25 14:42:05.970726 192.168.0.92 192.168.0.1 Modbus/TCP 66
                                                                   query [ 1 pkt(s)]: trans:
⊞ Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

⊕ Ethernet II, Src: Toshiba_5d:79:43 (00:23:18:5d:79:43), Dst: Pronet_d7:08:55 (
⊞ Internet Protocol Version 4, Src: 192.168.0.92 (192.168.0.92), Dst: 192.168.0.
⊞ Transmission Control Protocol, Src Port: afrog (1042), Dst Port: asa-appl-prot
■ Modbus/TCP
     transaction identifier: 0
     protocol identifier: 0
     length: 6
     unit identifier: 1
       function 4: Read input registers
       reference number: 0
       word count: 56
      00 20 4a d7 08 55 00 23
                                       5d 79 43 08 00 45 00
0000
                                                                 . J..U.# .]y⊂..E.
                                   75 f6 c0 a8 00 5c c0 a8 7f c9 00 0e ab 83 50 18
                                                                 .4. @... u...\..
      00 34 03 20 40 00 80 06
      00 01 04 12 01 f6 97 ee 7f c9 00 0e ab 83 50 18
ff od 81 d4 00 00 00 00 00 00 06 01 04 00 00
10020
0030
0040
      00 38
```

Example of TCP frame data:

000000000006010400000038

Breakdown of the above data:

0000 Transaction identifier 0000 Protocol identifier 0006 Length 01 Unit identifier 04 Function code 4 (0x04) 0000

Starting address

0038 Quantity of registers (0x0038=56dec)



a-2) From inverter to monitoring PC. Response to a-1

```
711 2012-05-25 14:42:05.972991 192.168.0.1 192.168.0.92 Modbus/TCP 175 response [ 1 pkt(s)]: trans:

⊕ Frame 11: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits)

⊞ Ethernet II, Src: Pronet_d7:08:55 (00:20:4a:d7:08:55), Dst: Toshiba_5d:79:43 (

⊕ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: afroq

■ Modbus/TCP
    transaction identifier: 0
    protocol identifier: 0
     length: 115
    unit identifier: 1
  function 4: Read input registers
      byte count: 112
      Data
      00 23 18 5d 79 43 00 20
00 a1 01 79 00 00 40 06
                                     d7
                                  4a
f7
0000
                                         08
                                            55
                                               08
                                                   00 45
                                                         00
                                                                         J..U..E.
                                        c0
97
                                               00
7f
                                            a8
                                                     <0
0010
                                     30
                                                   01
                                                         a8
                                                                         .0..
                f6 04 12
                                                   d5
                                                      50
0020
          5 C
             01
                          00 0e
                                     83
                                            ee
                                                         18
0030
      16
         d0 38 fa 00 00
                          00
                                  00
                                     00
                                         00
                                                   04
            01
08
      01
03
         00
0f
0040
                d6
                          01
                                     00
                                         00
                                            00
                                               01
                00 00 00 00
                                  ōö.
                                         00
                                            00
                                               00
0050
                             00
                                     00
                                                   00
                                                      00
         00 00 00 00 00 00 00
00 00 00 00 02 70 00
01 f4 07 e8 07 e2 07
                                     00 00
                                            00
13
38
                                               00
84
25
                                                   00
0060
      00
                                                      00
                                  00
                                  00
e7
      00
                                     00
                                                   00
                                                      00
0070
                                         00
      9c
cd
ff
0080
                                     38
                                        99
                                                   38
         14
0090
                2a
                    59
                       0a
                          11
                              0a
                                  Ob.
                                     00
                                        00 00
                                               00
                                                   00
                                                      00
             10
looao
```

Example of TCP frame data:

Breakdown of the above data:

Transaction identifier

0000

0000 Protocol identifier 0073 Length 01 Unit identifier 04Function code 70 Byte count 0001 Data Status 0001d6ce Time stamp (YYMMDD): 0x0001d6ce=120526 0001dbe4 Time stamp (hhmmss): 0x0001dbe4=121828 0000001 Reserved 0000 Alarm flag 04030f08 Status bit 1 00000000 Status bit 3 Word-0 00000000 Status bit 3 Word-1 00000000 Status bit 3 Word-2 00000000 Status bit 3 Word-3 00000000 Status bit 3 Word-4 00000000 Status bit 3 Word-5 00000000 Status bit 3 Word-6 00000000 Status bit 3 Word-7 00000270 Energy 00000000 Reserved 1384 Active power P



0000	Reactive power Q
ff9c	Power factor: 0xff9c=-100(-1.00)
01f4	Grid frequency (500: 50.0Hz)
07e8	Grid voltage UV
07e2	Grid voltage VW
07e7	Grid voltage WU
3899	Inverter output current U
3825	Inverter output current V
38e8	Inverter output current W
15cd	DC input power
141c	DC input voltage
2a59	DC input current
0a11	Potential to ground PE
0a0b	Potential to ground EN
0000	Reserved
0000	DC reverse current 1
0000	DC reverse current 2
ffffffa4	Reserved
0000	Reserved
0000	Reserved
00000000	Reserved
00000000	Reserved



b-1) From monitoring PC to inverter. Request while inverter is stopped

```
70 10 2012-05-25 14:34:07.206779 192.168.0.92 192.168.0.1 Modbus/TCP 66 guery [ 1 pkt(s)]: trans:
⊞ Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

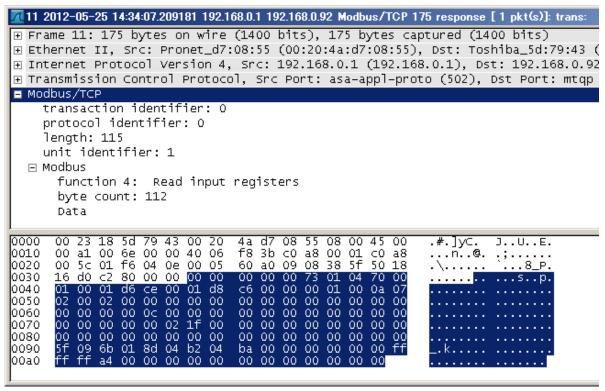
⊕ Ethernet II, Src: Toshiba_5d:79:43 (00:23:18:5d:79:43), Dst: Pronet_d7:08:55 (

⊕ Internet Protocol Version 4, Src: 192.168.0.92 (192.168.0.92), Dst: 192.168.0.

⊞ Transmission Control Protocol, Src Port: mtqp (1038), Dst Port: asa-appl-protc
Modbus/TCP
    transaction identifier: 0
    protocol identifier: 0
    length: 6
    unit identifier: 1
  function 4: Read input registers
      reference number: 0
      word count: 56
         20 4a d7
                                     5d 79 43 08 00 45 00
                                                                J..U.#
                                                                        .]y⊂.,E.
                                                              .4..@... x....\..
......<u>..</u> 85...\.P.
0010
      00 34 01 04 40 00 80 06
                                 78 12 c0 a8 00 5c c0 a8
                                 38 53 00 05 60 a0 50 18
10020
      00 01 04 0e 01 f6 09 08
      fa 53 81 d4 00 00 <mark>00 00</mark>
                                 00 00 00 06 01 04
10030
0040
```

Details omitted.

b-2) From inverter to monitoring PC. Response to b-1



Example of TCP frame data:

Breakdown of the above data

0000 Transaction identifier 0000 Protocol identifier 0073 Length



01 Unit identifier
04 Function code
70 Byte count
0001 Data status

0001d6ce Time stamp (YYMMDD) : 0x0001d6ce=120526 0001d8c6 Time stamp (hhmmss) : 0x0001d8c6=121030

00000001 Reserved

000a Alarm flag: 0x0a=0b00001010 (D03:Minor fault, D01:Grid fault)

07020002 Status bit 1 00000000 Status bit 3 Word-0 00000000 Status bit 3 Word-1 00000000 Status bit 3 Word-2 00000000 status bit 3 Word-3 000c0000 Status bit 3 Word-4 00000000 Status bit 3 Word-5 00000000 Status bit 3 Word-6 00000000 Status bit 3 Word-7

0000021f Energy: 0x21f=543...543kWh

00000000 Reserved 0000 Active power P 0000 Reactive power Q 0000 Power factor 0000 Grid frequency 0000 Grid voltage UV 0000 Grid voltage VW 0000 Grid voltage WU

0000 Inverter output current U 0000 Inverter output current V 0000 Inverter output current W

005f DC input power
096b DC input voltage
018d C input current
04b2 Potential to ground PE
04ba Potential to ground EN

0000 Reserved

0000 DC reverse current 1 0000 DC reverse current 2

fffffa4 Reserved 0000 Reserved 0000 Reserved 00000000 Reserved 00000000 Reserved



c-1) From monitoring PC to inverter. Communication error detection caused by internal circuit problem of the inverter

```
⊞ Frame 1438: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on into

⊕ Ethernet II, Src: Toshiba_11:d9:5b (e8:e0:b7:11:d9:5b), Dst: PronetGm_e6:bd:

⊞ Internet Protocol Version 4, Src: 10.1.1.92 (10.1.1.92), Dst: 10.1.1.167 (10
⊞ Transmission Control Protocol, Src Port: 49360 (49360), Dst Port: 502 (502),
■ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 1

    Modbus

    Function Code: Read Input Registers (4)
    Reference Number: 0
    Word Count: 56
0000
      00 20 4a e6 bd 38 e8 e0
                                 b7 11 d9 5b 08 00 45 00
                                                             . J..8.. ...[..E.
      00 34 0e 39 40 00 80 06
01 a7 c0 d0 01 f6 42 0f
                                                             .4.9@....\_.
0010
                                d5 86 0a 01 01 5c 0a 01
0020
                                 d1 40 00 00 c1 ed 50 18
                                                             ....В.
                                                                      .@....P.
      f5 3e 0a 37 00 00 <mark>00 00</mark>
                                00 00 00 06 01 04 00 00
0030
0040
```

Omitted below

c-2) From inverter to monitoring PC. Response to c-1

```
⊞ Frame 1439: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on int

⊕ Ethernet II, Src: PronetGm_e6:bd:38 (00:20:4a:e6:bd:38), Dst: Toshiba_11:d9:

⊕ Internet Protocol Version 4, Src: 10.1.1.167 (10.1.1.167), Dst: 10.1.1.92 (1)

⊞ Transmission Control Protocol, Src Port: 502 (502), Dst Port: 49360 (49360),
Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 3
    Unit Identifier: 1
Function 4: Read Input Registers. Exception: Gateway target device failer
    Exception Code: Gateway target device failed to respond (11)
                                 4a e6 bd 38 08 00 45 00
0000
      e8 e0 b7 11 d9 5b 00 20
                                                                        J..8..E.
                                                              . . . . . [ .
                                63 10 0a 01 01 a7 0a 01
c1 ed 42 0f d1 4c 50 18
      00 31 00 b3 00 00 40 06
0010
                                                              .1....@. c.....
      01 5c 01 f6 c0 d0 00 00 c1 ed 42 0f d1 4c 50 16 d0 dd 57 00 00 00 00 00 00 00 03 01 84 0b
                                                              .\....<u>..</u>.B..LP.
                                                              ...W...
0030
```

Example of TCP frame data:

00000000000301840b

Breakdown of the above data

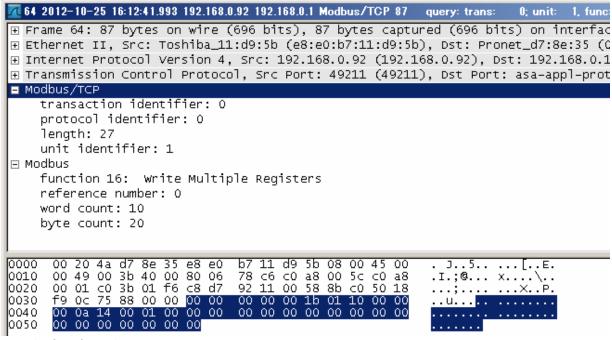
0000 Transaction ID 0000 Protocol ID 0003 Message length 01 Unit ID

84 Error code at exception response

Exception handling code at exception response 0b



- 5.2 Writing example for registers 40001~40010
- a-1) From monitoring PC to inverter. Stop command request



Example of TCP frame data:

Breakdown of the above data:

0000	Transaction identifier
0000	Protocol identifier
001b	Length
01	Unit identifier
10	Function code (0x10=16dec)
0000	Starting address
000a	Quantity of registers (0x000a=10dec)
14	Byte count (0x14=20dec)
0001	Operation (0x0001=1dec, Stop command)
0000	P limit enable/disable
0000	Active power P limit
0000	Q command enable/disable or power factor command enable/disable
0000	Reactive power Q command or power factor command
0000	Time Stamp Enable/Disable
00000000	Time Stamp(YYMMDD)
00000000	Time Stamp(HHMMSS)



a-2) From inverter to monitoring PC. Response to a-1

```
√ 65 2012-10-25 16:12:42.085 192.168.0.1 192.168.0.92 Modbus/TCP 66 response: trans:

                                                                             0; unit:
⊞ Frame 65: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interfac

    Ethernet II, Src: Pronet_d7:8e:35 (00:20:4a:d7:8e:35), Dst: Toshiba_11:d9:5b (ε

    Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.92

⊞ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: 49211
■ Modbus/TCP
     transaction identifier: O
     protocol identifier: 0
     length: 6
     unit identifier: 1
    function 16: Write Multiple Registers
     reference number: 0
     word count: 10
      e8 e0 b7 11 d9 5b 00 20
                                  4a d7 8e 35 08 00 45 00
                                                                          J..5..E.
      00 34 06 40 00 00 40 06 00 5c 01 f6 c0 3b 00 58
                                  f2 d6 c0 a8 00 01 c0 a8
8b c0 c8 d7 92 32 50 18
                                                                .4.@..@.
0010
0020
0030
      16 d0 6c ce 00 00 00 00 00 00 06 01 10 00 00
0040
      00 Oa
```

Example of TCP frame data:

00000000000601100000000a

Breakdown of the above data:

0000 Transaction identifier 0000 Protocol identifier 0006 Length

0006 Length01 Unit identifier

10 Function code (0x10=16dec)

0000 Starting address

000a Quantity of registers (0x000a=10dec)



b-1) From monitoring PC to inverter. Start command request

```
₹ 76 2012-10-25 16:12:53.347 192.168.0.92 192.168.0.1 Modbus/TCP 87 query: trans:
⊞ Frame 76: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interfac

⊞ Ethernet II, Src: Toshiba_11:d9:5b (e8:e0:b7:11:d9:5b), Dst: Pronet_d7:8e:35 (0)

⊕ Internet Protocol Version 4, Src: 192.168.0.92 (192.168.0.92), Dst: 192.168.0.1

    Transmission Control Protocol, Src Port: 49211 (49211), Dst Port: asa-appl-prot

■ Modbus/TCP
    transaction identifier: 0
    protocol identifier: 0
     length: 27
    unit identifier: 1
function 16: Write Multiple Registers
    reference number: 0
    word count: 10
    byte count: 20
      00 20 4a d7 8e 35 e8 e0
00 49 00 41 40 00 80 06
0000
                                 b7 11 d9
                                           5b 08 00 45 00
                                                                J..5.. ...[.,E.
                                 78 c0 c0 a8 00 5c c0 a8
0010
                                                              .I.A@... x....\..
      00 01 c0 3b 01 f6 c8 d7 f8 87 74 5b 00 00 00
0020
                                 92 3e 00 58 8c 45 50 18
                                                                        .>.X.EP.
0030
                                 00
                                     00
                                        00 1b 01
                                                  10
                                                     00
0040
                00 02
                       00 00 00
                                     00
0050
      00 00 00 00 00 00 00
```

Example of TCP frame data:

Breakdown of the above data:

Transaction identifier

0000

0000	Protocol identifier
001b	Length
01	Unit identifier
10	Function code (0x10=16dec)
0000	Starting address
000a	Quantity of registers (0x000a=10dec)
14	Byte count (0x14=20dec)
0002	Operation (0x0002=2dec, start command)
0000	P limit enable/disable
0000	Active power P limit
0000	Q command enable/disable or power factor command enable/disable
0000	Reactive power Q command or power factor command
0000	Time stamp enable/disable
00000000	Time stamp (YYMMDD)
00000000	Time stamp (HHMMSS)



b-2) From inverter to measurement PC. Response to b-1

```
77 2012-10-25 16:12:53.484 192.168.0.1 192.168.0.92 Modbus/TCP 66 response: trans:
 ⊞ Frame 77: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface

⊞ Ethernet II, Src: Pronet_d7:8e:35 (00:20:4a:d7:8e:35), Dst: Toshiba_11:d9:5b (e8)

    ⊕ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.92 (

    ⊕ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: 49211 (
 ■ Modbus/TCP
     transaction identifier: 0
     protocol identifier: 0
      length: 6
     unit identifier: 1
 function 16: Write Multiple Registers
     reference number: 0
     word count: 10
       e8 e0 b7 11 d9 5b 00 20
0000
                                   4a d7 8e 35 08 00 45 00
                                                                            J..5..E.
                                                                  . . . . . [ .
                                   f2 d2 c0 a8 00 01 c0 a8
8c 45 c8 d7 92 5f 50 18
       00 34 06 44 00 00 40 06
                                                                  .4.D..@. .....
       00 5c 01 f6 c0 3b 00 58 8c 45 c8 d7 92 5f 50 18 16 d0 6c 1c 00 00 00 00 00 00 06 01 10 00 00
10020
                                                                  .\...; <u>.X .E..._P.</u>
0030
0040
       00 Oa
Example of TCP frame data:
```

00000000000601100000000a

Breakdown of the above data: omitted



c-1) From monitoring PC to inverter. Active power P limit and reactive power Q command request.

```
₹ 157 2012-10-25 16:14:10.826 192.168.0.92 192.168.0.1 Modbus/TCP 87 query: trans:
⊞ Frame 157: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface
Ethernet II, Src: Toshiba_11:d9:5b (e8:e0:b7:11:d9:5b), Dst: Pronet_d7:8e:35 (00:

    ⊕ Internet Protocol Version 4, Src: 192.168.0.92 (192.168.0.92), Dst: 192.168.0.1 (

⊕ Transmission Control Protocol, Src Port: 49211 (49211), Dst Port: asa-appl-proto

■ Modbus/TCP
    transaction identifier: 0
    protocol identifier: 0
     length: 27
    unit identifier: 1
function 16: Write Multiple Registers
    reference number: 0
    word count: 10
    byte count: 20
      00 20 4a d7 8e 35 e8 e0
00 49 00 6d 40 00 80 06
0000
                                      11 d9
                                             5b 08 00 45 00
                                                                  J..5..
                                                                         ...[..E.
                                  78 94 c0 a8 00 5c c0 a8 93 2e 00 58 90 b6 50 18
                                                                .I.m@... x....\..
0010
0020
      00 01 c0 3b 01 f6 c8 d7
0030
      f9 f2 5a 83 00 00 00
                              00
                                  00
                                      00
                                         00
                                            1b
                                                01
                                                       00
                                                   10
                                            fb 2e
      00
00
          0a 14 00 03
00 00 00 00
l0040.
                       00
                           01
                                  e1
                                      00 01
                                                   00 00 00
                              10
0050
                       00
```

Example of TCP frame data:

Breakdown of the above data:

0000	Transaction Identifier
0000	Protocol Identifier
001b	Length (0x001b=27dec)
01	Unit Identifier
10	Function Code 16(0x10)
0000	Starting Address
000a	Quantity of Registers (0x000a=10dec)
14	Byte count (0x14=20dec)
0003	Operation (0x0003=3dec)
0001	P limit enable/disable (0x0001=1dec: P limit enable)
10e1	Active power P limit (0x10e1=4321dec: 432.1kW)
0001	Q command enable/disable or power factor command enable/disable (0x0001=1dec: Q command enable)
fb2e	Reactive power Q command or power factor command (0xfb2e=-1234dec: -123.4kvar)
0000	Time Stamp Enable/Disable
00000000	Time Stamp(YYMMDD)

00000000 Time Stamp(HHMMSS)



c-2) From inverter to monitoring PC. Response to c-1

```
/1 160 2012-10-25 16:14:10.932 192.168.0.1 192.168.0.92 Modbus/TCP 66 response: trans:
 ⊞ Frame 160: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface

⊞ Ethernet II, Src: Pronet_d7:8e:35 (00:20:4a:d7:8e:35), Dst: Toshiba_11:d9:5b (e8:

 ⊞ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.92 (1

    ⊕ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: 49211 (4)

 ■ Modbus/TCP
     transaction identifier: 0
     protocol identifier: 0
      length: 6
     unit identifier: 1
 function 16: Write Multiple Registers
     reference number: 0
     word count: 10
       e8 e0 b7 11 d9 5b 00 20
                                   4a d7 8e 35 08 00 45 00
                                                                           J..5..E.
                                                                 . . . . . [ .
       00 34 06 63 00 00 40 06
00 5c 01 f6 c0 3b 00 58
                                   f2 b3 c0 a8 00 01 c0 a8 90 b6 c8 d7 93 4f 50 18
                                                                 .4.c..@. .....
10010
10020
                                                                 .\<u>.</u>..;<u>.×</u>
0030
       16 d0 66 bb 00 00 00 00 00 00 06 01 10 00 00
0040
Example of TCP frame data:
```

Breakdown of the above data: omitted

00000000000601100000000a



d-1) From monitoring PC to inverter. Active power P limit and power factor command request

```
№ 176 2012-10-25 16:14:26.927 192.168.0.92 192.168.0.1 Modbus/TCP 87 query: trans:
                                                                                   0; unit: 1, func:
 ⊞ Frame 176: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface

⊕ Ethernet II, Src: Toshiba_11:d9:5b (e8:e0:b7:11:d9:5b), Dst: Pronet_d7:8e:35 (00:

    Internet Protocol Version 4, Src: 192.168.0.92 (192.168.0.92), Dst: 192.168.0.1 (

 ⊕ Transmission Control Protocol, Src Port: 49211 (49211), Dst Port: asa-appl-proto
 ■ Modbus/TCP
      transaction identifier: O
      protocol identifier: 0
      length: 27
      unit identifier: 1
 function 16: Write Multiple Registers
      reference number: 0
      word count: 10
      byte count: 20
       00 20 4a d7 8e 35 e8 e0
00 49 00 77 40 00 80 06
0000
                                         11 d9 5b 08 00 45 00
                                                                      J..5.. ...[.,E.
                                     78 8a c0 a8 00 5c c0 a8 93 67 00 58 91 b4 50 18
                                                                    .I.w@... x....\..
0010
       00 01 c0 3b 01 f6 c8 d7
f8 f4 e6 45 00 00 00 00
                                                                        <u>;</u>...<u>..</u>.g.X..P.
0020
                                     00 00
                                                1b 01
ff a1
                                                       10
0030
                                            00
       00 0a 14 00 03 00 01
00 00 00 00 00 00 00
0040
                                         00
0050
Example of TCP frame data:
```

Breakdown of the above data:

0000	Transaction Identifier
0000	Protocol Identifier
001b	Length
01	Unit Identifier
10	Function Code (0x10=16dec)
0000	Starting Address
000a	Quantity of Registers (0x000a=10dec)
14	Byte count (0x14=20dec)
0003	Operation (0x0003=3dec)
0001	P limit enable/disable (0x0001=1dec: P limit enable)
10e1	Active power P limit (0x10e1=4321dec: 432.1kW)
0002	Q command enable/disable or power factor command enable/disable
	(0x0002=2dec: Power factor command enable)
ffa1	Reactive power Q command or power factor command (0xffa1=-95dec: -0.95)
0000	Time stamp Enable/Disable
00000000	Time Stamp (YYMMDD)
00000000	Time Stamp (HHMMSS)



d-2) From inverter to monitoring PC. Response to d-1

```
№ 177 2012-10-25 16:14:27.031 192.168.0.1 192.168.0.92 Modbus/TCP 66 response: trans:
                                                                      0; unit: 1, func:
⊞ Frame 177: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface

⊞ Ethernet II, Src: Pronet_d7:8e:35 (00:20:4a:d7:8e:35), Dst: Toshiba_11:d9:5b (e8:

⊞ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.92 (1
■ Modbus/TCP
    transaction identifier: 0
    protocol identifier: 0
    length: 6
    unit identifier: 1
function 16: Write Multiple Registers
    reference number: 0
    word count: 10
0000
      e8 e0 b7 11 d9 5b 00 20
                              4a d7 8e 35 08 00 45 00
                                                         .....[.
.4.j..@.
                                                                  J..5..E.
                              f2 ac c0 a8 00 01 c0 a8 91 b4 c8 d7 93 88 50 18
      00 34 06 6a 00 00 40 06
00 5c 01 f6 c0 3b 00 58
10010
0020
0030
     16 d0 65 84 00 00 00 00 00 00 06 01 10 00 00
0040
     00 Oa
```

Breakdown of the above data: omitted



e-1) From monitoring PC to inverter. Example of time stamp setting request

```
17 303 2012-10-25 16:16:35.317005000 192.168.0.92 192.168.0.1 Modbus/TCP 87
                                                            query: trans:
                                                                        0; unit:
 ⊞ Frame 303: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface (

⊕ Ethernet II, Src: Toshiba_11:d9:5b (e8:e0:b7:11:d9:5b), Dst: Pronet_d7:8e:35 (00:20)

    ⊕ Internet Protocol Version 4, Src: 192.168.0.92 (192.168.0.92), Dst: 192.168.0.1 (19)

 transaction identifier: O
    protocol identifier: 0
     length: 27
    unit identifier: 1
 function 16: Write Multiple Registers
    reference number: 0
    word count: 10
     byte count: 20
0000
      00 20 4a d7 8e 35 e8 e0
                              b7
                                 11 d9 5b 08
                                            00 45 00
                                                               ...[..E.
                              78 47 c0 a8 00 5c
94 7e 00 58 98 ef
      00 49 00 ba 40 00 80 06
                                               c0 a8
0010
                                                       .I..@... xG...\..
      00 01 c0 3b 01 f6 c8 d7
0020
0030
      f7 a1 3e 71 00 00 <mark>00 00</mark>
                              00
                                 00
                                    00 1b
                                          01
0040
                 00
                    00
                       00
                                 00
                                    00
            14
                          00
      01
         d8 c1
              00 02
0050
                    0d
Example of TCP frame data:
 Breakdown of the above data:
 0000
         Transaction identifier
```

0000	Protocol identifier
001b	Length
01	Unit identifier
10	Function code (0x10=16dec)
0000	Starting address
000a	Quantity of registers (0x000a=10dec)
14	Byte count (0x14=20dec)
0000	Operation (0x0000=0dec)
0000	P limit enable/disable (0x0001=1dec: P limit disable)
0000	Active power P limit
0000	Q command enable/disable or power factor command enable/disable
	(0x0000=0dec: Q command disabled, power factor command disable)
0000	Reactive power Q command or power factor command
0001	Time stamp enable/disable(0x0001=1dec: Time stamp enable)
0001d8c1	Time stamp (YYMMDD) (0x0001d8c1=121025dec: 2012 October 25)
00020d64	Time stamp (HHMMSS) (0x00020d64=134500dec: 13:45:00



e-2) From inverter to monitoring PC. Response example to e-1

```
√0 304 2012-10-25 16:16:35.429327000 192.168.0.1 192.168.0.92 Modbus/TCP 66 response: trans:
 ⊞ Frame 304: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface

    ⊕ Ethernet II, Src: Pronet_d7:8e:35 (00:20:4a:d7:8e:35), Dst: Toshiba_11:d9:5b (e8:
 ⊞ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.92 (1
 ⊞ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: 49211 (4
      transaction identifier: O
      protocol identifier: 0
      length: 6
      unit identifier: 1
 function 16: Write Multiple Registers
      reference number: 0
      word count: 10
       e8 e0 b7 11 d9 5b 00 20
                                     4a d7 8e 35 08 00 45 00
0000
                                                                    . . . . . [ .
       00 34 06 9a 00 00 40 06 f2 7c c0 a8 00 01 c0 a8 00 5c 01 f6 c0 3b 00 58 98 ef c8 d7 94 9f 50 18 16 d0 5d 32 00 00 00 00 00 00 06 01 10 00 00
                                                                    .4....@.
                                                                              . | . . . . . .
                                                                    .\...;.× .....₽.
l0030
0040
       00 Oa
Example of TCP frame data:
```

Breakdown of the above data: Omitted

00000000000601100000000a

