ads-tec Industrial IT GmbH

IRF3000, IRF2000, IRF1000

Application Note
ModbusTCP API

Version 2.2

Inhaltsverzeichnis

1 Einführung

Modbus-TCP erlaubt es, das Verhalten eines Geräts über Ethernet von einer SPS aus zu steuern und Zustände abzufragen. Auf der Firewall können über dieses Protokoll die Verbindungsdienste (IPsec und OpenVPN) kontrolliert und CUT&ALARM quittiert werden.

Wenn zum Beispiel eine OpenVPN-Verbindung zwischen zwei Firewalls definiert und der Client als inaktiv konfiguriert wurde (siehe dazu den Usecase „OpenVPN“), dann kann der Client von einer SPS aus via Modbus-TCP aktiviert und damit die OpenVPN-Verbindung aufgebaut werden.

Dieser Application Note verwendet primär die IRF1000 als Beispiel, die dargestellten Einstellungen sind jedoch auf auch auf der IRF2000 oder IRF3000 identisch vorhanden.

Wichtige Hinweise:

- *Es kann sich nur eine SPS auf einmal mit dem Modbus-TCP-Dienst der Firewall verbinden.*

2 Hinweise zur IT-Sicherheit

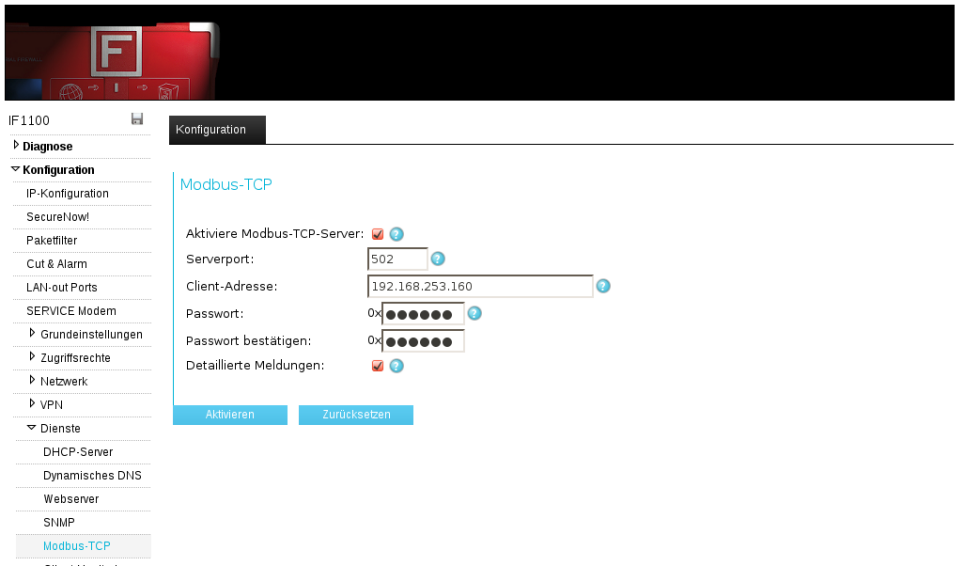
Modbus/TCP ist ein unverschlüsseltes und ungesichertes Protokoll! Es sollte daher nur in gesicherten Netzwerken verwendet werden!

Für den Betrieb dieser Funktion ist unbedingt darauf zu achten das der IP-Adressfilter auf das jeweilige sichere Netz konfiguriert wird!
Die verfügbare Passwortfunktion ist nur ein schwacher zusätzlicher Schutz und kann leicht umgangen werden, da die Dateninhalte unverschlüsselt übertragen werden oder die TCP-Session in einem Man-in-The-Middle Szenario übernommen werden kann!

Für eine sichere Verwendung dieser Funktion über ein ungesichertes oder nicht vertrauenswürdiges Netzwerk empfehlen wir das Verwenden eines VPN Kanals zum Gerät (OpenVPN, IPsec oder Big-LinX) und eine Einschränkung der zulässigen Quell IP-Adressen auf die IP-Adressen des VPN-Kanals.

3 Konfiguration

3.1 Modbus-TCP im Webinterface aktivieren



Unter `Konfiguration/Erweitert/Modbus-TCP` kann der Modbus-TCP-Server aktiviert werden. Zusätzlich können folgende Einstellungen getroffen werden:

- Der Serverport kann frei gewählt werden. Wird kein Port spezifiziert, wird auf dem Standardport für Modbus-TCP (502) auf eingehende Anfragen gewartet.
- Der Zugriff kann auf einen bestimmten Client beschränkt werden. Dazu kann die Client-Adresse als IP-Adresse mit Subnetzmaske in CDIR-Notation angegeben werden. Also z.B. 192.168.0.0/24 für das ganze Subnetz, oder 192.168.0.1/32 für eine einzelne Quelle. Wird keine spezielle Client-Adresse angegeben, kann die Verbindung von jedem Rechner aus erfolgen.
- Um die Sicherheit weiter zu erhöhen, kann ein 32-Bit-Passwort spezifiziert werden. Bevor ein Client auf die Status- und Inputregister zugreifen kann, muss er die höherwertigen 16 Bit in das „PASSWORD-HIGH“-Register 0x01 und die niederwertigen 16 Bit in das „PASSWORD-LOW“-Register 0x02 schreiben, falls ein Passwort gesetzt ist. Ansonsten kann er direkt auf alle Register zugreifen.
- Um den Eventlog nicht zu überfüllen, werden normalerweise nur wichtige Ereignisse oder Fehler gemeldet. Wird `Detaillierte Meldungen` aktiviert, werden zusätzliche Informationen zu Verbindungsaufbau und Anfragen geloggt.

Wichtige Hinweise:

- *Das Passwort wird überprüft, wenn der niederwertige Anteil in das Register 0x02 geschrieben wird. Lautet das Passwort zum Beispiel 0xaa11bb22, dann muss zuerst 0xaa11 in das Register 0x01 und anschließend 0xbb22 in das Register 0x02 geschrieben werden. Das Passwort gilt für die Dauer der TCP-Verbindung. Bei einem erneuten Verbindungsaufbau werden die Passwortregister auf 0x0000 zurückgesetzt.*
- *Das Passwort ist nur gültig für eine TCP-Verbindung. Jede neue TCP-Verbindung muss zuerst das Passwort neu schreiben.*
- *Das Passwort wird in Big-Endian Codierung ausgewertet.*

3.2 Aktivierung von OpenVPN

Um zum Beispiel einen OpenVPN-Eintrag zu aktivieren, der mit der OpenVPN-Schnittstelle L2-VPN1 assoziiert ist, muss die SPS mittels Funktionscode 0x10 den Register 0x24 auf den Wert 1 setzen. Wird das Register auf 0 gesetzt, wird der Eintrag deaktiviert und die Verbindung wieder abgebaut.

Wichtige Hinweise:

- *Das Inputregister enthält unabhängig vom Ergebnis der Aktion den zuletzt geschriebenen Wert (oder 0, falls das Inputregister bis dahin noch nicht geschrieben wurde). Der eigentliche Status der Verbindung muss aus dem entsprechenden Statusregister ausgelesen werden (für OpenVPN-1 zum Beispiel 0x14).*
- *Die anderen Inputregister arbeiten analog (mit Ausnahme von CUT&ALARM-Register 0x10, das nur auf 0x00 zum Quittieren der Meldungen gesetzt werden kann).*

3.3 Auslesen der Statusregister

Die SPS kann alle Statusregister in einer Anfrage abrufen. Dazu muss sie mittels des Funktionscodes 0x03 oder 0x04 von der Startadresse alle Register auslesen.

Wichtige Hinweise:

- *Aus Performanzgründen sollten die Statusregister nicht zu oft ausgelesen werden, sowie nur solche die wirklich benötigt werden. Die Register werden jeweils „On-Demand“ mit aktuellen Daten gefüllt! Die Antwortzeit des Gerätes kann daher erheblich variieren!*

4 Modbus/TCP Register Spezifikation

4.1 Grundlegendes

Die Modbus-TCP-Implementierung basiert auf der offiziellen Dokumentation der Modbus-IDA Independent User Organization (http://modbus.org):

- http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf
- http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

Auf der IRF1000, IRF2000 und der IRF3000 läuft ein Modbus-TCP-Server, der Anfragen auf dem TCP-Port 502 (falls nicht anders konfiguriert) entgegennimmt.

Folgende Funktionscodes können vom Modbus-TCP-Server verarbeitet werden:

- 0x03 (Read Holding Registers)
- 0x04 (Read Input Registers)
- 0x06 (Write Single Register)
- 0x10 (Write Multiple Registers)

Die Leseoperationen 0x03 und 0x04 sind in ihrem Verhalten identisch.
In den nachfolgenden Erklärungen steht Bit 0 für das niederwertigste und Bit 15 für das höchstwertigste Bit des Registers.

Sollte bei der Verarbeitung einer Anfrage ein Fehler auftreten, sind folgende Ausnahmecodes möglich:

0x01	Ungültiger Funktionscode	Weder 0x03, noch 0x04, noch 0x10 wurde als Funktionscode verwendet.
0x02	Ungültiges Register	Entweder existiert das Register nicht oder die gewünschte Operation kann nicht ausgeführt werden.
0x03	Ungültiger Registerwert	Der zu schreibende Wert ist ungültig für den Register.
0x04	Server-Fehler	Bei der Verarbeitung der Anfrage ist ein interner Fehler aufgetreten.

Wichtiger Hinweis: *Die Implementierung ist nicht zeitoptimiert. Der Aufbau einer OpenVPN-Verbindung kann zum Beispiel ungefähr 10 Sekunden dauern. Das Auslesen aller Statusregister in einer Anfrage kann ungefähr 5 Sekunden dauern. Dementsprechend lange braucht eine Antwort des Modbus-TCP-Servers. Aus*

Performanzgründen dürfen die Anfragen also nicht zu schnell erfolgen (insbesondere sollte der Status höchstens einmal die Minute abgefragt und auf die notwendigen Register beschränkt werden) und müssen die Timeouts der SPS hoch genug sein. Des Weiteren darf sich nur ein Client auf einmal mit dem Modbus-TCP-Server der Firewall verbinden.

4.2 Registerübersicht

Allgemeine Register:

- 0x00 (VERSION)
- 0x01 (PASSWORD-HIGH)
- 0x02 (PASSWORD-LOW)

Status-Register:

- 0x10 (CUT&ALARM)
- 0x11 (reserviert)
- 0x12 (reserviert)
- 0x13 (IPsec)
- 0x14 (OpenVPN-1)
- …
- 0x1D (OpenVPN-10)
- 0x1E (Big-LinX VPN)

Input-Register:

- 0x20 (CUT&ALARM)
- 0x21 (reserviert)
- 0x22 (reserviert)
- 0x23 (IPsec)
- 0x24 (OpenVPN-1)
- …
- 0x2D (OpenVPN-10)
- 0x2E (Big-LinX VPN)

Status-Register können nicht geschrieben werden. Für alle verbindungsspezifischen Status-Register ist der Inhalt ähnlich:

- Bit 0 enthält, ob die Verbindung überhaupt definiert ist, also entweder ein Eintrag existiert oder der Dienst aktiviert ist.
- Bit 1 enthält, ob die Verbindung aktiviert wurde.
- Bit 2 enthält, ob die Verbindung tatsächlich besteht.
- Die weiteren Bits geben typ-spezifische Informationen an.

Input-Register können gelesen und geschrieben werden. Solange wie der entsprechende Dienst eines verbindungs-spezifischen Registers nicht aktiv beziehungsweise nicht konfigurierbar ist, ist jeder Schreibversuch ungültig und es wird der Ausnahmecode 0x02 (Ungültiger Register) zurückgegeben. Unabhängig vom Erfolg einer durch das Schreiben eines Inputregisters ausgelösten Aktion, wird der Wert in den Inputregister geschrieben und kann ausgelesen werden. Der eigentliche Status des entsprechenden Dienstes muss aus dem Statusregister abgefragt werden.

4.3 Allgemeine Register

4.3.1 Version (Register 0x00)

Hier wird der Stand der Registerbeschreibung widergespiegelt. IRF2000 bis Version 4.1.8, IRF1000 bis Version 2.1.11 und IRF3000 bis Version 1.0.3 melden hier immer 0x0100. Für diese Firmwareversionen bitte die ältere Version dieses Dokuments verwenden. Neuere Versionen (auf welche sich dieses Dokument bezieht) melden 0x0101
Das Register kann gelesen aber nicht geschrieben werden. Das höherwertige Byte ist die Major- und das niederwertige Byte die Minorversionsnummer.
Eine SPS-Implementierung welche mit den verschiedene Version korrekt umgehen muss kann dieses Register zur Umschaltung des Verhaltens verwenden.

4.3.2 Password (Register 0x01 und 0x02)

Register 0x01 (PASSWORD-HIGH) ist der höherwertige Teil und Register 0x02 (PASSWORD-LOW) der niederwertige Teil des 32-Bit-Passworts. Beide Register können normal geschrieben und gelesen werden. Falls ein Passwort verlangt wird, muss dieses korrekt gesetzt werden, bevor auf die Status- und Inputregister zugegriffen werden kann. Die Passwortverifizierung wird durchgeführt, sobald der Register 0x02 geschrieben wird (Register 0x01 muss also als erstes gesetzt werden). Das Passwort gilt für die gesamte Dauer der TCP-Verbindung. Bei einem erneuten Verbindungsaufbau wird der Inhalt beider Register auf Null zurückgesetzt.

4.4 CUT&ALARM

Hinweis: Geräte ohne CUT&ALARM wie die IRF1000 liefern für Lesezugriffe auf diese Register immer den Wert 0 sowie eine Modbus Exception bei Schreibzugriffen.

4.4.1 Status (Register 0x10)

Bits	Bedeutung	Erklärung
0	ALARM	ALARM ist aktiv
1	Interner CUT	CUT ist aktiv
2	Externer CUT	CUT ist aktiv
3-15	Unbenutzt	

4.4.2 Control (Register 0x20)

Der Register kann mit dem Wert 0x0000 beschrieben werden, um ALARM und internen CUT zu quittieren. Der externe CUT kann auf diesem Weg nicht zurückgesetzt werden, da es sich um ein anliegendes Signal handelt. 0x0000 ist der einzig erlaubte Wert.

4.5 IPsec

4.5.1 Status (Register 0x13)

Bits	Bedeutung	Erklärung
0	Verbindung ist startbereit	Mindestens ein Tunnel ist bereit. (Variable: ipsec_conn_[0-64]_status != „disabled“)
1	Dienst ist aktiviert.	IPsec ist global aktiviert
2	Verbunden	Mindestens ein Tunnel ist aufgebaut
3	Deprecated	
4	Deprecated	
5	Deprecated	
6-7	Reserved	
8-15	Deprecated	

4.5.2 Control (Register 0x23)

Das Register kann entweder mit dem Wert 0x0001 (Verbindung aktivieren) oder mit dem Wert 0x0000 (Verbindung deaktivieren) beschrieben werden. Die jeweilige IPsec Verbindung müssen als „geschaltet“ konfiguriert sein! Es werden immer alle IPsec-Verbindungen gestartet oder gestoppt für welche dies zutrifft.

4.6 OpenVPN

4.6.1 Status (Register 0x14-0x1D)

Bits	Bedeutung	Erklärung
0	Definiert	Der OpenVPN-Eintrag existiert
1	Aktiviert	OpenVPN-Eintrag ist aktiviert
2	Verbunden	Tunnel ist aufgebaut

3	Master	Der Eintrag ist als Master konfiguriert
4-7	Unbenutzt	
8-15	Clients	Anzahl der Clients (nur Master)

4.6.2 Control (Register 0x24-0x2D)

Das Register kann entweder mit dem Wert 0x0001 (Eintrag aktivieren) oder mit dem Wert 0x0000 (Eintrag deaktivieren) beschrieben werden, falls der Eintrag definiert ist.

4.7 Big-LinX

Diese Register sind erst ab Firmware 4.2.0 (IRF3000), 1.3.0 (IRF1000) und 1.0.5 (IRF3000) verfügbar!

4.7.1 Status (Register 0x1E)

Bits	Bedeutung	Erklärung
0	WWH Status	1: WWH ist Online, 0: WWH ist Offline
1	Aktiviert	Big-LinX VPN ist als permanent konfiguriert ohne Quittierung und ohne Schaltung.
2	Verbunden	1: Der Tunnel ist aktuell aufgebaut, 0: Der Tunnel ist aktuell nicht aufgebaut
3	Quittierung erforderlich	Der Tunnel wartet auf Quittierung
4	Wartend	Der Tunnel ist konfiguriert, Smartcard oder Zertifikat ist bereit. Tunnel ist bereit für VPN-Aufbau.
5	Verbindung aktiviert	Die Verbindung wurde aktiv geschalten / es wird versucht sie aufzubauen / sie ist aufgebaut / es wird auf die Quittierung gewartet.
6	reserved for future use	
7	reserved for future use	

4.7.2 Control (Register 0x2E)

Das Register kann entweder mit dem Wert 0x0001 (Big-LinX VPN aktivieren) oder mit dem Wert 0x0000 (Big-LinX VPN deaktivieren) beschrieben werden.
Voraussetzung ist, dass eine gültige PIN im Gerät gespeichert ist – sofern nötig - oder ggfs. ein Software-Zertifikat ausgerollt wurde.

Für den Fall, dass die Quittierung der VPN Kanals via API aktiv ist kann mit m Wert 0x02 die Quittierung gesetzt werden.