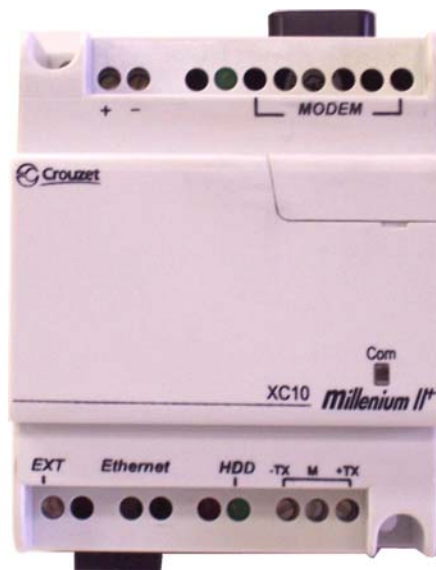


Created on 03/02/2007
Rev. 1.5

WEB Server

Millenium II — *Web Server*



The MIIWeb User Guide

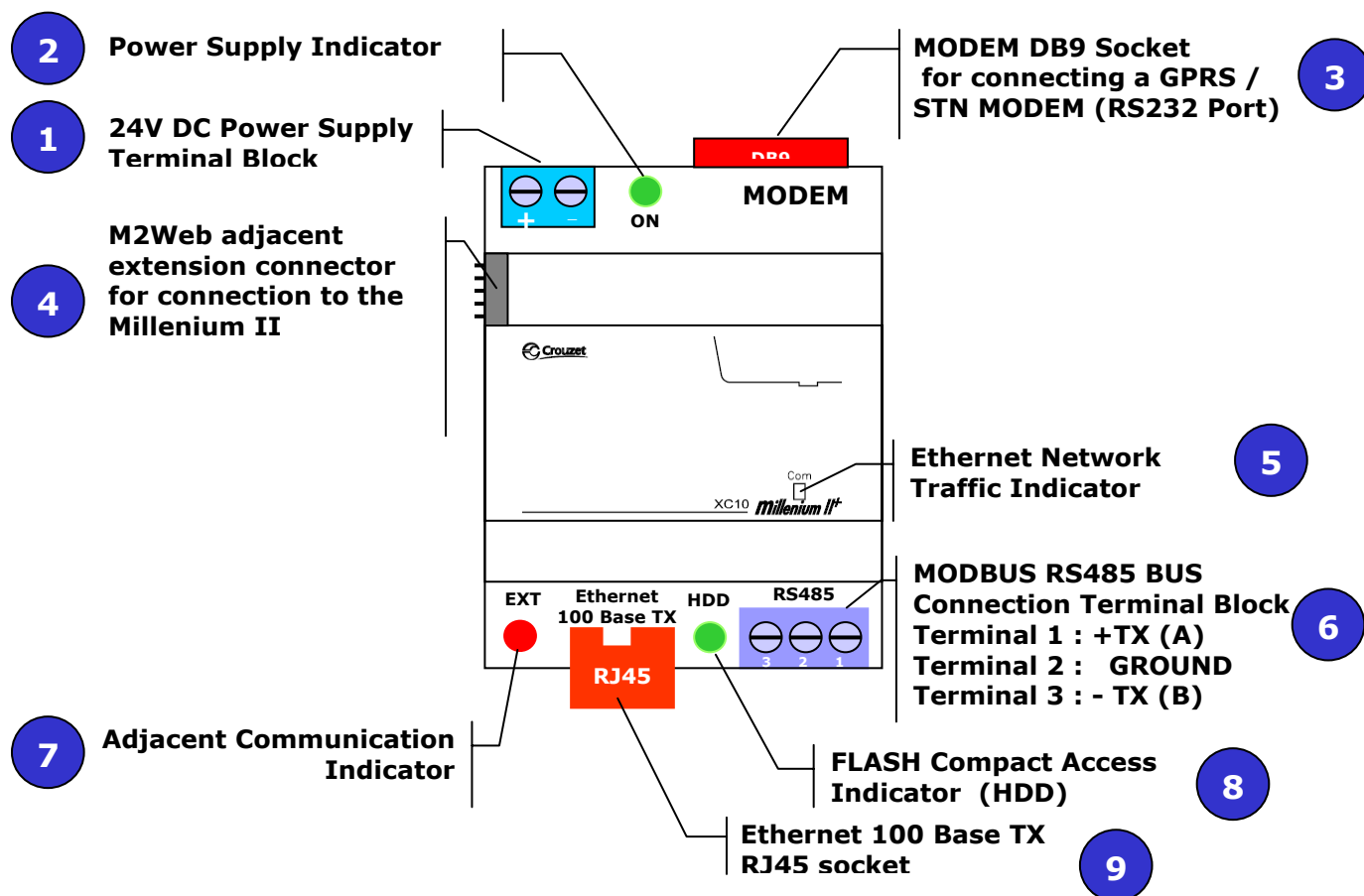
CONTENTS

I - Wiring and Precautions for Use	4
I.1.1 - Physical Appearance of the MII Web Server	4
I.1.2 - Connection to an RTU MODBUS Network	5
I.1.3 - Connection to the Millenium II as an Adjacent Extension.....	7
I.1.4 - Power Supply	9
I.1.5 - Connection to the Ethernet Network	10
I.2 - <i>MIWeb's Network Functions</i>	11
II - Configuration Using the eTiceSoft Software	13
II.1 - Introduction.....	13
II.1.1 - What is eTiceSoft.....	13
II.1.2 - Conditions for Installation	13
II.1.3 - Installation	13
II.2 - Creating a New Project.....	14
II.2.1 - Defining a Project	14
II.2.2 - Constituent Elements	14
II.3 - Configuring a Project.....	15
II.3.1 - Hardware Configuration Page	15
II.3.2 - RTU MODBUS Parameters	16
II.3.3 - System Clock	16
II.3.4 - Registering the Milleniums Connected to MIWeb.....	17
II.3.5 - MODEM Parameters	18
II.3.6 - Information and Malfunctions	21
II.3.7 - Network Services.....	22
II.3.8 - Creating the Configuration File.....	24
III - WEB Navigation	25
III.1 - Connecting to the Web Server	25
III.1.1 - Introduction.....	25
III.1.2 - Making the WEB Connection	25
III.1.3 - Starting a Session	27
III.2 - Menu Bar.....	29
III.2.1 - The Navigation Menu.....	29
III.2.2 - Connection Data.....	29
III.2.3 - Date and Time	30
III.3 - The Monitoring Page	30
III.3.1 - Selecting the Flow Chart.....	30
III.3.2 - Utilisation and Limits.....	31
III.4 - The Remote Maintenance Page	31
III.5 - The Configuration Pages	32
III.5.1 - The Configuration Panel.....	32
III.5.2 - Advanced Configuration of the WebServer.....	36
III.6 - The Logbook	43
III.7 - The Archiving Page	44
III.7.1 - The Graph Zone	44
III.7.2 - The Disk Space Measurement Zone	46
IV - Events	47
IV.1 - Definition.....	47
IV.2 - Limitations	47

IV.3 - Progress of a Scan Cycle: Critical Case.....	48
IV.4 - Condition for Triggering the Action for an Event.....	49
V - Description and Technical Characteristics.....	50
V.1 - Hardware Aspects	50
V.1.1 - Connection.....	50
V.1.2 - General Characteristics	50
V.2 - Communication Characteristics.....	51
V.2.1 - Network Services (using TCP /IP)	51
V.2.2 - UDP Services	54
V.2.3 - Security of the TCP/IP Transactions	55
V.2.4 - Communication via RTU MODBUS	57
V.2.5 - Dialogue with the Millenium	58
V.2.6 - Data Exchange by MODEM.....	59
V.2.7 - Alarms.....	60
V.2.8 - Archiving	61
VI - Maintenance	61
VI.1 - Maintenance operations	61
VI.1.1 - Free disk space management.....	61
VI.1.2 - Updating the Web Server	64
VI.2 - Important notices	65
VI.2.1 - Powering	65
VI.2.2 - Using a MODEM	65
VI.2.3 - Using MODBUS	66
VI.2.4 - WebServer TCP/IP security notes	67
VI.3 - Critical use cases	67
VI.3.1 - MODEM RS232 link broken without any PPP connection in progress	67
VI.3.2 - MODEM or ISP link broken during a PPP Client connection	68
VI.3.3 - MODEM or PPP Client link broken during a PPP Server connection.....	68
VI.3.4 - Powerfail during or after an eTiceSoft data transfer.....	69
VI.3.5 - MODBUS Slave malfunction	69
VI.3.6 - Static Disk is full (HDD Full).....	70
VI.3.7 - System clock is not synchronised	70

I - Wiring and Precautions for Use

I.1.1 - Physical Appearance of the MII Web Server



1 : 24 V DC Power Supply Terminal Block: The power supply shall provide a voltage ranging between 12 V and 30 V DC for a peak current of 400 mA.

2 : Power Supply Indicator : When the MIIWeb is powered, this indicator is illuminated.

3 : Male DB9 MODEM Socket : RS232 connector for external MODEM (only signals RTS, CTS, TXD, RXD and the ground are connected to the connector pins)

4 : Adjacent Extension Connector : Using an interconnection strip, the MIIWeb becomes an adjacent extension for a Millenium II, in which MIIWeb is registered as an XC10 M2WEB Module.

5 : Network Traffic Indicator : This red indicator lights up every time the MIIWeb detects or outputs a frame on the Ethernet segment to which it is connected (connection via item 9).

6 : MODBUS Connection Terminal Block: MIIWeb is connected to the RTU MODBUS – RS485 Field bus via this 3-pin connector. It must be located at one of the ends of the network (Line termination resistance included)

7 : Adjacent Communication Indicator : When the MIIWeb exchanges data with the adjacent Millenium connected using connector 4, this indicator flashes every 500ms.

8 : HDD Indicator : This indicator lights up when the MIIWeb writes to or reads its static hard disk. It indicates filing activity or that consultation is on-going.

9 : RJ45 Socket: RJ45 connector for unshielded UTP – FTP Ethernet category 5 cable.

I.1.2 - Connection to an RTU MODBUS Network

MIIWEB is a MODBUS **master** WEB server, it communicates with all the 3-wire, 8-bit RTU MODBUS slaves having an exchange table consisting of single words (16 bits). (e.g. : TSX PLCs, Milleniums, TWIDO, Frequency drives, slave Millenium displays (MAGELIS XBT)...).

MIIWEB operates on RTU MODBUS via RS485 connection. In this configuration it is theoretically possible to connect 31 slaves at a distance of up to 1200m.

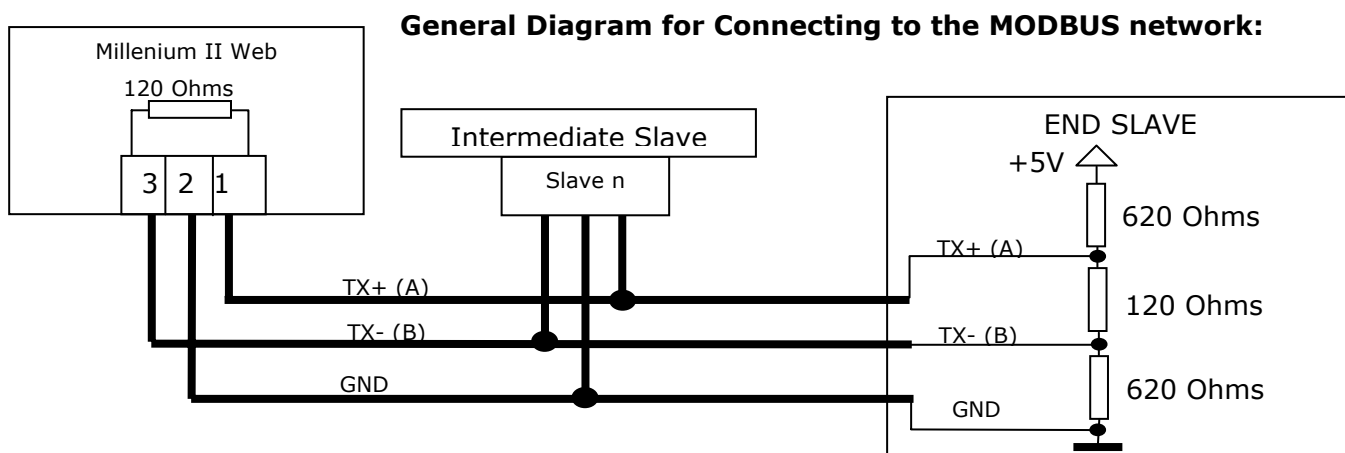
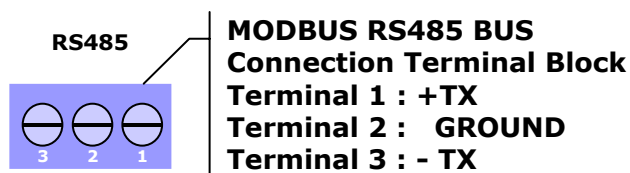
Each slave is identified on the BUS by an address which must be unique (between 1 and 254).

So MIIWEB is the **sole network master**, its role is to interrogate the slaves or to send them commands using the functions defined in the RTU MODBUS protocol (mainly uses functions 3 and 16 of the RTU MODBUS protocol).

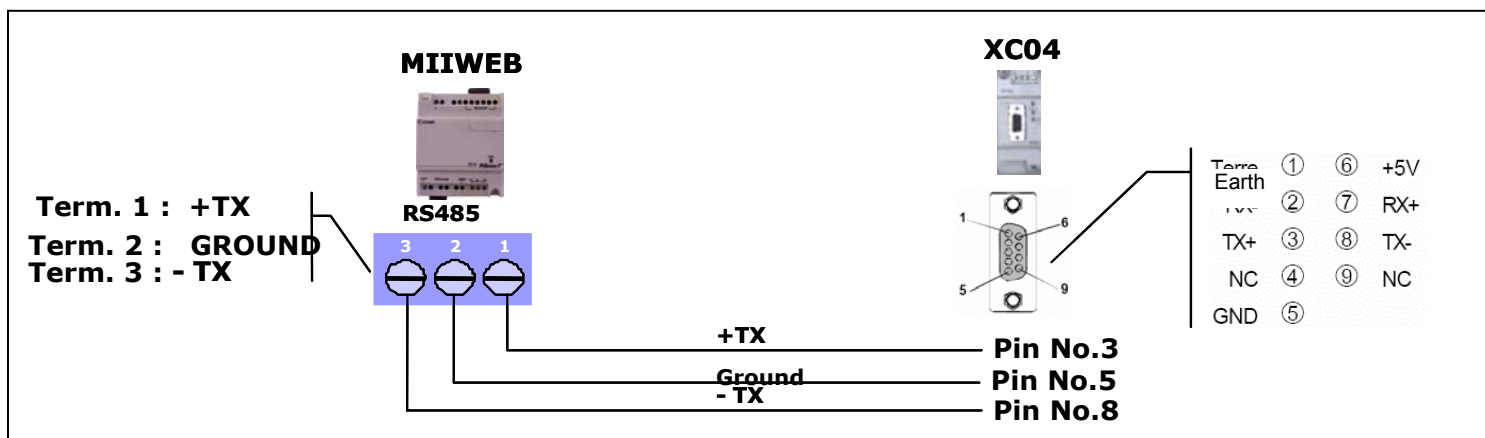
The maximum transmission rate accepted by the Milleniums is 57600 Bauds, but the recommended rate is 19200 Bauds (default value).

It is mandatory that all the items of equipment connected to the RTU MODBUS network driven by the MIIWEB be SLAVES.

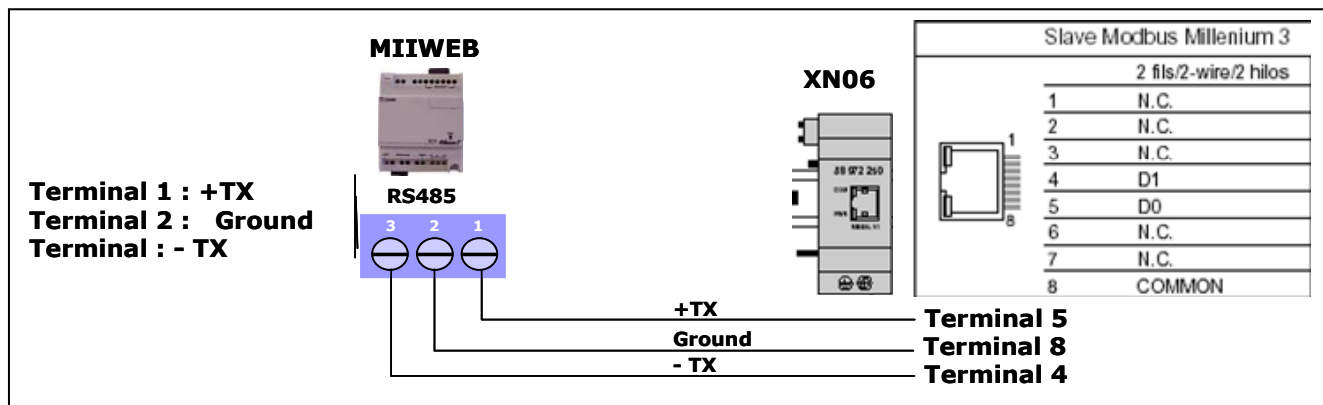
The MODBUS network is connected to the MIIWEB via a 3-wire terminal block.



Connection to an XC04 module :



Connection to an XN03 or XN06 (Millenium 3) module :



Electrical Characteristics of the RTU MODBUS Connection

- Impedance between lines : 120 Ohms (line termination resistance included)
- Electric lines without opto-isolation, protected against 100V peak surges for 10μs.
- Maximum range: 1200m on an RS485 RTU MODBUS network fitted with 31 slaves with a maximum load impedance corresponding to the specifications of the MODICOM - RTU MODBUS implementation standard on a serial RS485 line.
- Available transmission rate in bauds: 300 to 57600 bauds.

Wiring Precautions

It is preferable to install the MIIWeb at one of the ends of the MODBUS – RTU – RS485 field bus since the line match resistors are incorporated and not accessible to the user (permanently connected).

MIIWeb does not have RS485 line polarisation resistors, it must be connected to a slave on the MODBUS network (preferably to the last).

RTU MODBUS protocol limitations

The RTU MODBUS network must comply with the following conditions:

Transmission rate : from 300 bauds to 57600 bauds

Data format : 1 Start bit, 1 Stop bit, 8 Data bits

Parity bit : Even, Odd, None.

Physical support: RS485 only (2-wire link : TX+ and TX-).

Restricted to exchange tables with one 16-bit word for reading or writing.
(Impossible to access double words)

NOTE :

For the MIIWeb to communicate via the MODBUS network, it must be told where the data is to be written to or read from; the eTiceSoft software provides for this.

MIIWeb can only communicate with a total of 8 Millenium at the most, since Millenium data is processed specifically by MIIWeb in order to optimise the transfer time.

I.1.3 - Connection to the Millenium II as an Adjacent Extension

MIIWeb is capable of dialoguing with a Millenium II connected as an adjacent extension, it must be registered as **XC10 – M2web** in the Millenium workshop (the XC10 catalogue entry is created on installing the eTiceSoft program).

The MIIWEB server extension is connected to the adjacent lateral extension of the « Millenium II » logic controllers in the **XT20 range only** via a pin connector:



Configuration from the M2 Software Workshop

From the « **Crouzet M2 Software** » program, follow the procedure below :

Procedure :

- 1 – Click on « New »



- 2 – Click on the Millenium « **XT 20** » image

- 3 – Select the P/N for the Millenium for your application from the list below

Type	Référence	Entrées	Sorties
XT20 R 24VDC	88950061	4 TOR + 8 TOR/ANA	1 RELAIS INV + 7 RELAIS...
XT20 S 24VDC	88950062	4 TOR + 8 TOR/ANA	6 PWM/TOR + 2 TOR
XT20 R 100-240VAC	88950063	12 TOR	1 RELAIS INV + 7 RELAIS...
XT20 R 24VAC	88950064	12 TOR	1 RELAIS INV + 7 RELAIS...
XT20 R 12VDC	88950065	4 TOR + 8 TOR/ANA	1 RELAIS INV + 7 RELAIS...
XT20 S 12VDC	88950066	4 TOR + 8 TOR/ANA	6 PWM/TOR + 2 TOR
XT20 RN 24VDC	88950069	8 TOR-NPN + 4 TOR/ANA	1 RELAIS INV + 7 RELAIS...

- 4 – Select the type of Millenium extension by clicking on « **XC** »

Choix du type de contrôleur et extensions associées

Type du contrôleur

XT20 R 24VDC
88950061 - 4 TOR + 8 TOR/ANA - 1 RELAIS INV + 7 RELAIS NO
avec compteur rapide

Extensions associées

Type	Référence	Entrées	Sorties
XC			
XL			

- 5 – Click on « **XC10 M2 WEB** »

Choix d'une extension

Type	Référence	Entrées	Sorties
XC01 4E/2S 24VDC	88950210	4 TOR	2 RELAIS NO
XC02 ASI 24VDC	88950213	5 TOR	6 TOR
XC03 MODBUS 24VDC	88950214	8 TOR + 3 ENTIERS	8 TOR + 3 ENTIERS
XC04 MODBUS 24VDC	88950823	8 TOR + 3 ENTIERS	8 TOR + 3 ENTIERS
XC10 M2 WEB	88950124	8 TOR + 3 ENTIERS	8 TOR + 3 ENTIERS

- 6 – Click on « **OK** » to validate the configuration

Type du contrôleur

XT20 R 24VDC
88950061 - 4 TOR + 8 TOR/ANA - 1 RELAIS INV + 7 RELAIS NO
avec compteur rapide

Extensions associées

Type	Référence	Entrées	Sorties
XC: XC10 M2 WEB	88950124	8 TOR + 3 ENTIERS	8 TOR + 3 ENTIE...

Addresses of the MODBUS data words

XC10 Module Words Used by MIIWeb

a – Write Word

MODBUS Address in the Millenium	Corresponding Address on the MODBUS Network
I1XC .. I8XC : b0, b1, b2, b3, b4, b5, b6, b7, b8	0 : b0, b1, b2, b3, b4, b5, b6, b7, b8
I9XC : 16-bit word	1
I10XC : 16-bit word	2
I11XC : 16-bit word	3

b – Read Word

MODBUS Address in the Millenium	Corresponding Address on the MODBUS Network
O1XC O8XC : b0, b1, b2, b3, b4, b5, b6, b7, b8	10 : b0, b1, b2, b3, b4, b5, b6, b7, b8
O9XC : 16-bit word	11
O10XC : 16-bit word	12
O11XC : 16-bit word	13

c- Write Read Words : The 7 Clock Words

The MII Web WebServer synchronises its system clock on the first Millenium registered in its internal list (registered using eTiceSoft). It then exchanges the real-time clock data in the Millenium II using the MODBUS XC10, XC03 or XC04 exchange words provided for this purpose; this occurs on initialisation, and then from time to time (around every 5 minutes at the most).

The Web Server also provides for resetting the time remotely on all the Milleniums connected to it (refer to Chapter : WEB Navigation).

Comments :

MIIWeb is capable of accessing **each individual bit** of the XC0-11 I/O words, through an internal masking algorithm which has been specially optimised for the Millenium II.

I.1.4 - Power Supply

The MIIWeb WebServer only withstands voltages ranging from +12 V DC to +30VDC and absorbs a peak current of up to 400mA with 24V DC applied.

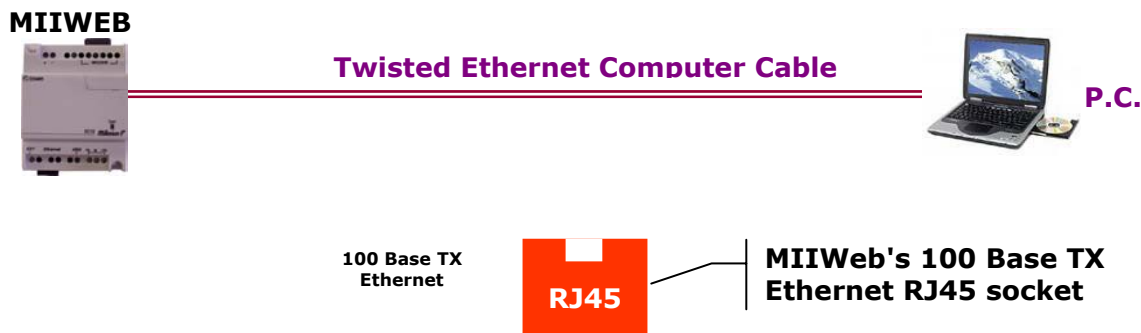
Reversing the polarity is not destructive for the device, but may short circuit the installation's power supply.

Surges above 30V DC or AC such as connecting 230V AC mains to the unit's power supply terminal block for example, will DESTROY IT immediately and definitively.

1.1.5 - Connection to the Ethernet Network

a) Connection via a twisted cable : Direct PC link to the MIIWeb WebServer

This is the easiest and fastest means of testing the MIIWeb's operation, or of programming it. This connection method makes it possible to access the data contained in the MIIWeb very quickly.



When the MIIWeb is connected, the network traffic indicator LED flashes during TCP/IP packet transactions between the PC and the WebServer.

N.B. :

In this case, the WebServer's DHCP client has to be deactivated in most cases (because the PC and the WebServer are both DHCP clients waiting for a server address). It is preferable to allocate the IP addresses manually (refer to eTiceSoft).

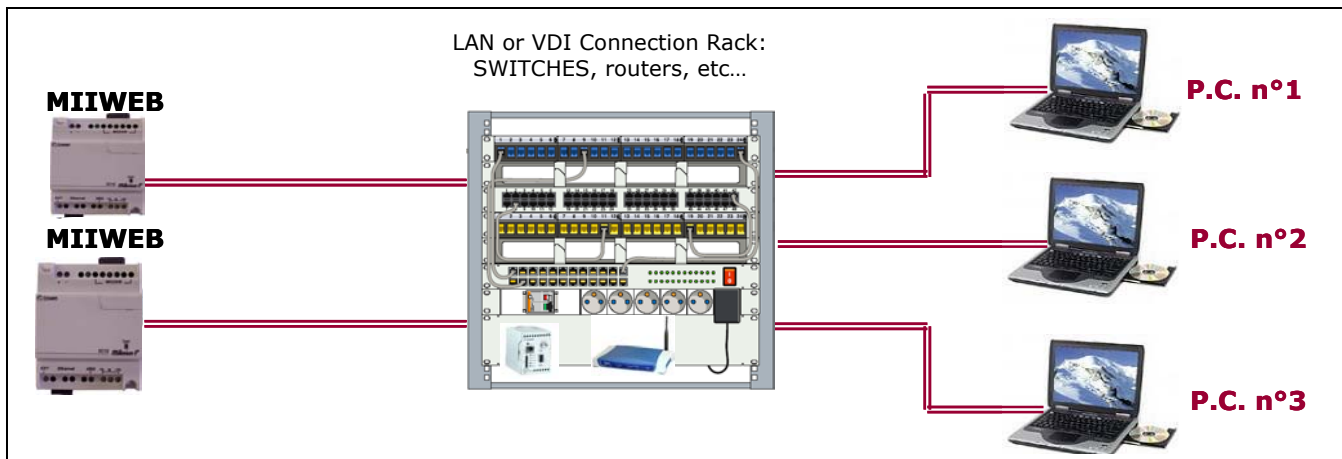
b) Integration in a LAN (Local Area Network)

In this configuration, the WebServer is connected to the local network using a distribution box (SWITCH or HUB) or a Router in the case of LAN/WAN interconnection (Connection to the ADSL network via a Modem/Router).

This is certainly the configuration most frequently encountered, and requires that particular attention be paid to the IP addressing range in the network, which often has a DHCP Server. Where this is the case, the Web Server's DHCP client enables it to configure itself automatically (IP parameters, DNS Servers ...)

The WebServer is then connected to the LAN (or VDI network) via a non-twisted FTP Ethernet cable which must be at least category 5.

At this point the MIIWeb can be consulted and accessed from any LAN workstation.



I.2 - MIIWeb's Network Functions

Network Service	Activation	Port Used	Function
WEB Server	Always active	By default 80 (http) Can be changed in administrator session	Consulting the WebServer via the Internet
FTP Server	Activation /deactivation in Administrator Web session	By default 21 (FTP) Can be changed in administrator session	Downloading files / Modifying monitoring and configuration pages from eTiceSoft
TELNET Server	Activation /deactivation in Administrator Web session	By default 23 (TELNET) Can be changed in administrator session	Terminal mode, useful for real-time diagnostics on the operations performed by MIIWeb
DHCP Client	Activation /deactivation in Administrator or Supervisor Web session or on LAN if UDP 8001 port open from eTiceSoft	UDP Port 68	Automatic IP parameter allocation : auto-configuration in LAN or behind an ADSL router (e.g. : Netgear DG834G).
SMTP Client	Only used if the project sends eMails and if an SMTP server is accessible from the LAN or through the gateway.	Port 25	Messaging service Enables MIIWeb to send eMails to an SMTP message server which is not secured by a password
DNS Client	Used if the primary or secondary DNS parameters are operational and accessible to the LAN via the gateway.	Port 53	Enables MIIWeb to contact a Provider's SMTP messaging server where only its domain name is given, or to contact the DynDNS server, when the DynDNS client attempts to refresh a URL for the MIIWeb.
UDP Config Server	Used by eTiceSoft on a LAN to configure MIIWeb	UDP Port 8001	Updating the firmware. Changing the IP address. Automatic detection on the LAN network.
DynDNS Client	Used if the DNS servers exist and are operational. Can be activated / deactivated from eTiceSoft or Advanced Configuration in Administrator session	Outgoing Port 80	Provides for connecting to a Dynamic domain name server to advise it of a change in IP address (for Dynamic IP addresses provided by Internet Providers or GPRS network APNs)

PPP Client	Activated /deactivated from eTiceSoft, connection to a PPP server which can be activated from the Supervisor or Administrator session	All MIIWeb ports once the connection to the Provider's or GPRS APN's PPP server is made.	Provides for connecting to an Internet Provider via an analog MODEM, or to an APN offered by a GPRS wireless telephone operator.
PPP Server	Activated / deactivated with eTiceSoft, and triggered if a PPP client attempts to connect to the DATA (GSM) or telephone line to which the MODEM connected to the MIIWeb is connected. This service is only active if a client PPP connection or SMS transmission is not on-going on the MIIWeb.	All MIIWeb ports once the connection has been made by the remote PPP client.	Enables one single PC to connect to the PPP server incorporated in MIIWeb via a GPRS or STN modem.

II - Configuration Using the eTiceSoft Software

II.1 - Introduction

II.1.1 - What is eTiceSoft

The MIIWeb WebServer is designed to be configured by people who are not computer specialists, and who have no specific skills in programming in HTML, JAVA, FLASH or other structured languages which are usually inevitable when implementing WebServers in a control command architecture.

The eTiceSoft software workshop provides for producing and grouping all the MIIWeb WebServer design and configuration procedures from a single Windows application.

This application provides for :

- editing and compiling animated and dynamic vectorial monitoring flow charts which can be consulted using any Internet navigator capable of running the Macromedia / Adobe FlashPlayer™ PlugIn (MAC OS, Linux, Unix, Windows...)
- configuring the MIIWeb WebServer functions : Network services, managing the MODBUS network, configuring events, etc...
- transferring or downloading remotely, via a TCP/IP Network, the files containing all the new parameters.
- downloading archive files in the same way as with any other FTP client
- updating the MIIWeb WebServer firmware should a new issue be released,
- detecting and configuring remotely (on a LAN) the IP parameters of the WebServer, even if they are not compatible with the LAN in which it is incorporated (this very useful function is nonetheless rarely encountered on this type of equipment).
- creating and enriching the visual component libraries, through an integrated component editor.

II.1.2 - Conditions for Installation

The eTiceSoft software workshop is compatible with Windows 2000, Windows XP, and Windows NT operating systems.

It requires 30Mo of available disk space,

A screen with at least 1024 x 768 pixels, SVGA or better
256 Mo RAM.

Having a local hard disk designated **C** : on which Windows is installed and with the **Program Files** directory.

If the above conditions are not met, the eTiceSoft software workshop will not be able to operate properly.

II.1.3 - Installation

Installing the software creates a directory called eTice in the Program Files folder, and in which a sub-directory eTiceSoft is created. The eTiceSoft.exe application is the executable file to which the desk shortcuts and Windows Start menu direct the system.

II.2 - Creating a New Project

II.2.1 - Defining a Project

A project in eTiceSoft software workshop terms is a set of files intended to produce the data necessary for configuring and using an MIIWeb.

A project has a name and corresponds to a folder set up by the eTiceSoft software at a given location of a storage peripheral (usually a hard disk). All the files used by eTiceSoft (except for the bitmap images used by the monitoring interfaces) are stored in this folder.

The project has an identification file (*.etp), containing all the paths to all the files comprising the project, as well as other parameters.

To be useable by MIIWeb, a project must be compiled and transferred into an MIIWeb.

The compilation procedure is performed once the project is loaded by simply clicking on the compilation button :



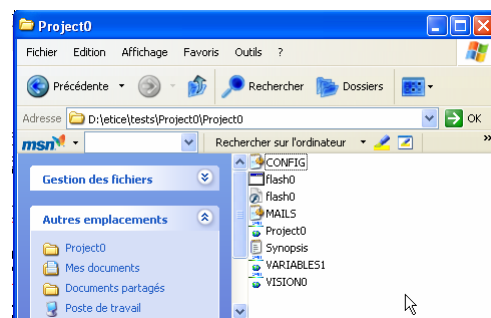
This operation generates all the files needed by MIIWeb and which will need to be downloaded, and groups them in the project directory.

The file downloading phase is performed using a tool incorporated in the eTiceSoft software workshop. This Downloading Manager provides for detecting the MIIWeb devices connected to a LAN or registering new ones, configuring their IP addresses remotely, then for downloading these files. This tool is also capable of updating the firmware of an MIIWeb should this be necessary.

II.2.2 - Constituent Elements

A project folder consists of the following elements:

- the configuration file : config.ini
- the event file : mails.ini
- the flow chart definition files :
 - ✓ *.htm,
 - ✓ *.swf,
 - ✓ vision*.*
- the compilation summary file : synopsis.txt
- the project definition file : *.etp



Only some of these files are effectively transferred into an MIIWeb after compilation.

II.3 - Configuring a Project

II.3.1 - Hardware Configuration Page

Each eTiceSoft project must contain a configuration. This may be defined when the project is first started or before it is compiled.

The configuration window is shown below :

Advanced configuration of the WebServer

MODBUS RTU Parameters
 MODBUS Baudrate: 57600 bps Parity: Even Advanced settings
 System clock source: Millenium #1

Declaration of Milleniums connected to WebServer
☐ Connected as contiguous extension (Millenium II only)
☒ Connected on MODBUS RTU (RS485)
 Add to List
 Millenium's extension type: XN03 (Millenium 3)
 MODBUS Address of the Millenium: 1
☒ Reset registers IXC or IXN for each new project transfer or reboot

Id	Connecté à	Type	Adresse
1	EXTENSION	Millenium II	
2	MODBUS	XC04 (Millenium II)	5
3	MODBUS	XN06 (Millenium 3)	7
4	MODBUS	XN06 (Millenium 3)	8

MODEM Parameters (for SMS and PPP Connections)
☒ **Activate PPP Server**
 Select the MODEM: GPRS-WAVECOM:FASTRACK(M1306B)
 RS232 parameters for communication with the MODEM
 Baudrate: 115200 Bauds
 Hardware flow Control RTS/CTS: ☒

PPP Client parameters
 PIN Code of the SIM Card: 0000
 PUK Code of the SIM Card (if locked):
 Phone number of the PPP Internet Provider: *99***1#
 LOGIN: PASSWORD:
 PPP Authentication Method: PAP
 GPRS APN (only for GPRS MODEM):
 Connection program: Never

Informations and Malfunctions (Faulty Millenium connections, enable to archive, or other system informations)
 If MODEM, Phone Number of the person to be notified: +330000
 If service activated, eMail address of the person to be notified: MrX@fai.fr
 Sending a SMS for internal alarm: ☐
 Use history file (LOGFILE.TXT): ☒

Network services
 Company's Mail address: Societe@fai.fr
☒ eMail service active (SMTP Client)
☒ DNS Client
☐ DynDNS Client (Dynamic DNS)
 Parameters of the eMail Server (SMTP Server)
 Domain Name of the SMTP Server: monfai@smtp.fr
 IP Address of the SMTP Server: 0 . 0 . 0 . 0
 DNS Servers parameters
 Primary DNS IP Address: 0 . 0 . 0 . 0
 Secondary DNS IP Address: 0 . 0 . 0 . 0

Cancel Create the configuration file and put it in UpLoad list

The various fields provide for filling in the WebServer system services.

The window is essential for specifying the connections and network services used, and for informing the WebServer of the Millenium devices with which it will be exchanging data from time to time (date, time, XC words, remote maintenance...).

II.3.2 - RTU MODBUS Parameters

These parameters must be identical for all the RTU MODBUS peripherals connected to that field network.

MODBUS Transmission rate: from 300 bauds to 57600 bauds (default value: 19200 bps)

Parity bit : None, Even, Odd

II.3.3 - System Clock

The WebServer does not provide a powersave internal system Clock. On the powering, it then needs to synchronise its internal system clock with the one integrated in one of the device connected to the WebServer.

In fact, the WebServer is able to synchronise its system clock using two ways selected with the field "**System Clock Source**" in the configuration panel of eTiceSoft workshop:

- If at least one Millenium is connected to the WebServer and correctly declared in the project, then the WebServer can synchronise its system clock to the Millenium's real time system clock. In that case the first Millenium declared in the list will be used for System Clock synchronisation automatic procedure. You need to choose this solution to select "Millenium 1" in the field's ComboBox.
- If no Millenium is used in the application project, then, it's possible to read date and time data from an other MODBUS Slave connected to the Modbus field BUS identified by its Slave address (ex. : Twido, PLCs...), with the condition that the data are structured and correctly formatted with right MODBUS Slave Registers address defined below :

Slave Clock data	Data Word address in the MODBUS Slave	Format	
		MSB (8bits)	LSB (8bits)
Secondes / Seconds	h0020 / 32d	00	XX(0-59)
Minutes / Minutes	h0021 / 33d	00	XX(0-59)
Heures / Hours	h0022 / 34d	00	XX(0-23)
Jour / Day	h0023 / 35d	00	XX(1-7)
Date / Date	h0024 / 36d	00	XX(1-31)
Mois / Month	h0025 / 37d	00	XX(1-12)
Année / Year	h0026 / 38d	00	XX(00-99)

Comment: These words are read and used by WebServer for its system clock synchronisation on WebServer's start sequence and periodically (every 100 system cycles) using MODBUS Functions 0x03 (Read Multiple Registers (only one request for the 7 Words)).

II.3.4 - Registering the Milleniums Connected to MIIWeb

MIIWeb is optimised for fast data management and communication with the Millenium logic controllers.

At each scan cycle, MIIWeb interrogates in succession the Milleniums registered with it and in the order in which they were registered.

In general, it is mandatory that all the MODBUS devices connected to the MIIWeb be configured as slaves, each with a unique address. This rule which is inherent to the RTU MODBUS network specifications also applies to the Millenium devices connected to the MIIWeb which is consequently the only master in the network.

There are two solutions for connecting a Millenium to an MIIWeb :

- 1 - Using the MIIWeb WebServer's RTU MODBUS network
- 2 - By connecting the MIIWeb WebServer directly to the adjacent extension connector of a 24VDC Millenium II XT20.

Registering the Milleniums connected to an MIIWeb consists in generating an exhaustive list specifying the type of the connection (adjacent or MODBUS) used to communicate with the Millenium, and for MODBUS connections, the slave address of the XC03, XC04, XN03 or XN06 Module of the Millenium concerned.

Comment: a Millenium connected as an adjacent extension is managed on priority, so it is systematically placed at the top of the registration list.

The Milleniums registered in a project must be configured and physically connected to the MIIWeb before the latter is configured or initialised. Otherwise, the MIIWeb will indicate connection faults once its initialisation is complete.

Comment:

Only Milleniums need to be registered in this list, the other MODBUS slave devices connected to the WebServer do not need to be registered beforehand in the project.

The events or monitoring objects whose behaviour depends on a MODBUS slave other than a Millenium are automatically interrogated by the MIIWeb once the project has been compiled.

The MIIWeb exchanges data with the Millenium devices using the exchange words IX, OX and clock words to read or write 16-bit words.

If the MIIWeb connection is via the MODBUS network, MIIWeb uses the MODBUS addresses for these words depending on the type of extension: XC03, XC04, XN03 or XN06.

If connection to the MIIWeb is by the adjacent extension connector on the Millenium II, then MIIWeb uses the functions of the Millenium II extension BUS protocol.

Whenever power is cut off from or a project loaded in the MIIWeb, the IX write exchange words are retained "as is".

It is possible a priori for IX exchange words to become desynchronised, since MIIWeb retains in memory the latest change to the IX/OX exchange words made since its initialisation.

To limit the impact of this effect, the Web Server can force all the IX words in all the Milleniums connected (including the adjacent Millenium) to be reset to zero on each re-initialisation, power up, or every time a project is loaded.

This function is activated if the box shown below is checked:

☐ **Reset IXC words to zero on each new project transfer**

Comments:

It is possible to add Milleniums to or delete them from the registration list in an existing project. But in this case, the events or monitoring objects whose behaviour depends on those Milleniums have to be modified manually and exhaustively by the person in charge of these modifications.

II.3.5 - MODEM Parameters

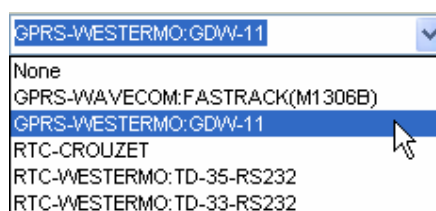
a) Select the MODEM

The Millenium II Web WebServer is capable of driving different types of MODEM, using an appropriate AT command sequence. Since the MODEMS on the market have different functions, some initialisation sequences may differ from one unit to another. So the MIIWeb has to use the right MODEM driver.

These drivers are text files (*.GSM) which contain all the commands needed by the MIIWeb to drive a given MODEM. They are incorporated in the project if a MODEM is effectively used, then transferred to the remote MIIWeb.

The software workshop searches automatically for the MODEM drivers available on the PC's hard disk, and updates the list of MODEMS compatible with MIIWeb.

Select the appropriate MODEM from the scrolling list



b) Activating / Deactivating the PPP Server

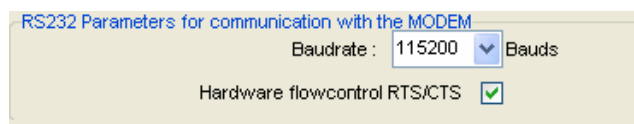
MIIWeb incorporates a PPP server, which enables it to make a Peer-to-Peer connection embodying TCP/IP with a remote client using an analog line. In this case, MIIWeb behaves like a Server which will be called by the client using the telephone number of the line to which the MODEM is connected.

To activate this server, check the corresponding box:



Comment: If the PPP server is active, the phase automatically initialising and synchronising the MIIWeb with the MODEM connected to it may take some time (5 minutes at the most).

c) MODEM and RS232 Parameters



MIIWeb communicates with the MODEM using a simplified RS232C serial link. Only the signals: CTS, RTS, TX, RX and the ground are connected to the unit's Sub-D 9-pin male connector.

In order to ensure good transmission reliability, depending on the length of the cables and the desired data transmission rate, the RS232 transmission rate can be selected (from 300 bauds to 115200 bauds) and RTS/CTS hardware flow control can be activated or deactivated.

By default, the optimum parameters are: Binary flow rate: 115 200 bauds, hardware flow control activated.

Do not change these parameters unless your MODEM or your configuration absolutely requires you do to so.

d) SIM Card Parameters

SIM Card parameters	
PIN Code of the SIM card	<input type="text" value="0000"/>
PUK Code of the SIM card (if locked)	<input type="text"/>

If the MODEM connected is of the GPRS type (and only in this case), communication can only be made if a valid SIM card is present in the MODEM.

It is essential that this SIM card, activated by a wireless telephone operator, be activated by a secret code termed PIN code.

This 4-figure code must be entered before using the MODEM, so the MIIWeb which initialises the MODEM every time it is re-started, has to know the code.

This is why it is PRIMORDIAL that the PIN code field for the SIM card is filled in.

If by accident, the PIN code given by the MIIWeb connected to the MODEM, is entered wrongly three times in succession, the SIM card locks up and can no longer be used as is.

The owner of the telephone subscription then has to contact his operator to obtain another code, called a PUK code, to unlock the SIM card.

MIIWeb can unlock the SIM card automatically, but to do so, it has to have the PUK Code. If this field is not filled in, MIIWeb will not be able to unlock the SIM card if there is an error in the PIN code number.

So the PUK code field is optional.

e) PPP Client Parameters

MIIWeb also incorporates a PPP client, capable of connecting automatically to a Provider (Internet Access Provider), using an STN or GPRS MODEM.

The Internet Access Provider is accessible by means of a telephone number, which MIIWeb will have to dial (or via an APN), and of an authentication procedure specific to PPP networks.

PPP Provider's Telephone Number: This field must contain the telephone number that MIIWeb must dial to access the Provider's PPP server.

Comments :

- If the MODEM is a GPRS MODEM, connecting to the Internet via MIIWeb's PPP client may be made via an APN. The APN's telephone number is often replaced by the following code: ***99***1#**
- It is IMPERATIVE that the APN name be specified in the field reserved for the **GPRS Operator's APN**

When a subscription to the Internet is taken out, the Provider gives a set of access codes which are necessary to make a PPP connection with its PPP server. These codes are needed during the PAP or CHAP authentication phases requested by the PPP server (to make the TCP/IP connection in PPP).

The **PPP Authentication Method** (PAP or CHAP) used by the PPP server to make the connection must also be specified from the corresponding scrolling list.

The request for PPP client connection, including the time frame, can be programmed by selecting an option from the **Connection** scrolling list :

- **Permanent (from power up)** : once it has succeeded in synchronising and initialising the MODEM connected to it, from the moment power is applied or after each re-start, MIIWeb attempts to make a client PPP connection with the specified Provider's PPP server. if the liaison is interrupted (loss of the carrier, disconnection from the PPP server...) from time to time MIIWeb attempts to make the client PPP connection again (every 5 minutes maximum).

The time frame is defined by entering a Connection Start and End time:

Connection start at 0 H 0 min End: 0 H 0 min

Comment :

If the connection start and end times are the same, then the PPP client will only attempt to connect when an eMail is to be sent and if no other route to the SMTP server is accessible (e.g. : via Internet router).

- **Periodic, or when mails are to be sent** : from time to time over a given time frame, MIIWeb attempts to connect to the specified Provider's PPP server. Outside this time frame the PPP client may attempt to make a connection to use the network services offered by the Provider to send an eMail related to an MIIWeb event. If the PPP client connection is not made, the eMail cannot be sent and a fault is notified.
- **Never** : The PPP client is deactivated. So it is impossible to connect to the Provider's PPP server even if any Mails need to be sent.

II.3.6 - Information and Malfunctions

MIIWeb manages a logbook. It writes all the important operations or malfunctions which occur in the log in chronological order :

- ✓ Power up,
- ✓ MODEM initialisation,
- ✓ PPP client and server initialisation,
- ✓ Unable to send an eMail or an SMS,
- ✓ Communication faults with the Milleniums or other MODBUS peripherals,
- ✓ Failure on network transactions,
- ✓ The times at which users connect/disconnect, and their sessions...

Some important events in the log are of great importance and have high priority, they may trigger an alarm. Such alarms may cause a Mail or an SMS to be sent to a single priority addressee identified by his telephone number (capable of receiving SMS) and his eMail address.

Logbook events likely to trigger an alarm are as follows :

Alarm	Triggered by	Message
Wake up	WebServer Initialisation	WebServer xxxx is online at IP Address xxx.yyy.www.zzz.
HDD Failure	Fault on accessing archive file	Cannot open Archive file
Millenium MODBUS error	Communication fault with MODBUS Millenium	Cannot exchange with Millenium #xi (MODBUS Address: y)
ADJACENT Millenium error	Communication fault with adjacent Millenium	Cannot exchange with Adjacent Millenium (#x)

If box "**Send an SMS on internal alarm**" is checked, then the system attempts to send both an SMS and an email to warn the person identified.

The logbook can be recorded in a text file named logfile.txt. This file contains all the log notifications. It is in the tab-tab-return format, and has to be reinitialised from time to time (limited disk space).

It is accessible and can be downloaded from a normal FTP client or from eTiceSoft connected to MIIweb's FTP server.

The LOGFILE.TXT file is updated if the box « **Use the history file (LOGFILE.TXT)** » is checked.

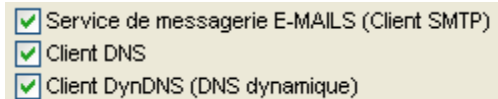
II.3.7 - Network Services

MIIWeb can communicate with several types of network services :

- Domain name server (DNS),
- Dynamic domain name server (DynDNS)
- SMTP message server.

This section of the configuration window in the eTiceSoft software workshop provides for filling in the corresponding clients for the MIIWeb WebServer.

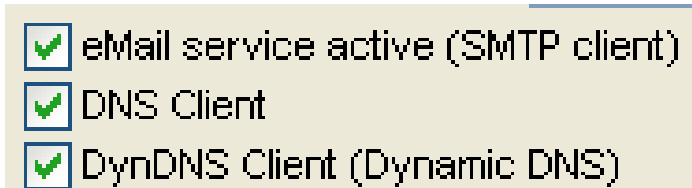
The services can be activated or deactivated by checking the corresponding boxes in the configuration window :



a) SMTP Client

It is **IMPERATIVE** that the « **Company eMail Address** » field be filled in with a valid message address no more than 29 characters long. This address will identify the origin of an eMail sent by the MIIWeb WebServer.

This address is essential for SMTP message servers which **check its validity** before accepting the eMail message attached to it. If the address is not valid or does not exist, the eMail issued by MIIWeb will usually not be transmitted !



The **SMTP Server Domain Name** enables the server to be identified on the Internet network by its domain name; this domain name may not be more than 69 characters long.

Further more, the domain name can only be used by MIIWeb if the latter has access to a valid DNS service (DNS servers accessible and correctly configured).

If the DNS name resolution services are not accessible, you have to know the IP address of the SMTP server which MIIWeb will have to contact to leave an eMail message. In this case, that IP address must be specified in the **SMTP Server IP Address** field.

If the DNS service is operational, MIIWeb will automatically update the SMTP server's IP address using its domain name, and filling this field in becomes optional.

b) DNS Client

MIIWeb is capable of connecting to the DNS domain name resolution server. This service enables a domain name (or URL) to be converted into an IP address. This function is used by MIIWeb to :

- Access an SMTP server : to send an eMail, each time an attempt to send an eMail is made, MIIWeb searches for the most recent IP address corresponding to the SMTP server, and to do this, it connects to the DNS server to obtain it.
- Access a DynDNS server : to inform the DynDNS server of a change of address. This DynDNS server is identified by a domain name (e.g. : members.dyndns.org/nic/update).

The DNS service is accessible via redundant Servers, intended to respond reliably to a name resolution request. This service is much in demand, and may occasionally be swamped. For this reason, Providers often make two DNS servers available to their subscribers, to ensure optimum service quality. The two servers are identified by two distinct IP addresses termed Primary DNS and Secondary DNS.

The Provider often gives the IP addresses of both these servers to its subscribers.

Comments :

In the case of a client PPP connection, and if the PPP server authorises it (which it usually does), MIIWeb can obtain the IP address of these DNS servers automatically, from the moment the client PPP connection is made. They will be used in addition to the servers normally accessible via the Ethernet network.

The address of these PPP DNS servers then appears in the MIIWeb's configuration panel, by way of information.

Where a DHCP server is used, MIIWeb can, in certain circumstances, detect automatically the IP addresses of the DNS servers. This function, although it is very practical in the case of a well-structured network, can however be inefficient should the DHCP server be wrongly configured or its parameters be invalid or incorrectly refreshed. The DHCP server must also be capable of transmitting DNS parameters (which is not always the case).

c) Dynamic DNS Client

MIIWeb is capable of indicating its IP address to a dynamic domain name resolution server (DynDNS).

This useful function makes it possible to find the public IP address of an MIIWeb, even if it changes (Dynamic IP address), from a domain name (e.g. : mywebservetest.dnsalias.com).

To be able to use this function, it is IMPERATIVE that the DNS service be activated.

An account must be opened with a DynDNS entity, in order to have an unique domain name, with which the dynamic public address enabling an MIIWeb to be accessed at a given moment will be associated. Within certain limits, this service is free; it becomes payable beyond a given number of accounts. The best known DynDNS entity is the www.DynDNS.org association.

Comment :

MIIWeb connects periodically to its server to refresh the DynDNS account's IP address. This client connection is achieved using outgoing port 80 on the TCP/IP protocol. So this port has to be open to the network firewalls for this service to operate. If the port is blocked or busy, MIIWeb cannot connect to the DynDNS service, making it impossible to refresh the IP address.

Description of the fields to be configured :

Dynamic DNS Client (uses Outgoing TCP Port 80)

DynDNS Server URI	<input type="text" value="members.dyndns.org/nic/update"/>	DynDNS Account	
		LOGIN :	<input type="text" value="test"/>
Host name of M2Web :	<input type="text" value="m2Web.dyndnsalias.com"/>	PASSWORD :	<input type="text" value="test"/>

DynDNS Server URL: this field enables MIIWeb to access the management account for the dynamic IP addresses for the DynDNS Service provider. So this field must contain the complete domain name for the DynDNS update server. Where a DynDNS entity account is used (www.DynDNS.org), this domain name is as follows :

members.dyndns.org/nic/update.

The maximum length of the domain name for the DynDNS update server must not be more than 99 characters.

MIIWeb Domain Name: this field tells the DynDNS server the domain name to which the MIIWeb concerned must notify its new IP address.

This is the domain name that the user registered with the DynDNS entity and which he will subsequently use to access this MIIWeb on the Internet.

LOGIN : this field contains DynDNS session Username. Every time a connection is made to the DynDNS service, this session name is requested by the server to access the DynDNS account. The LOGIN is determined when the DynDNS account is opened.

PASSWORD : a Password is associated with a DynDNS session name (LOGIN), and is necessary to access the domain name account. This password is determined by the subscriber to the DynDNS service when the account is created.

II.3.8 - Creating the Configuration File

All the above configuration data for a project are stored in a text file called **config.ini** which will be located in the directory for the current project.

Once the project has been compiled, this config.ini file will be loaded into the remote MIIWeb, where the firmware will then analyse and decode it.

To create the **config.ini** file, click on the « Create the file and put it in the downloading list » button.

Pressing the « Cancel » button does not change the **config.ini** file if it already exists, it simply closes the configuration window.

Comment :

If no project is open, the config.ini file is created in the last project directory opened or under the root c :.

III - WEB Navigation

III.1 - Connecting to the Web Server

III.1.1 - Introduction

MIIWeb is an embedded Internet Server, which means that it accepts client connections capable of interpreting and using the **http 1.0 (Hyper Text Transfer Protocol)** protocol.

Client software programs making connections under the HTTP protocol are usually Internet Navigators.

To be able to operate with MIIWeb, these navigators have to be compatible with the Adobe/Macromedia FLASH Player™ PlugIn. This small program is designed to display complex animated objects defined using mathematical algorithms based on vectorial definition.

This freeware is downloaded (and often already installed) in most navigators which have already been used to surf the Internet.

If this Plug-in is not installed, it can be downloaded directly from the Macromedia site :

http://www.macromedia.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash

Animated objects in monitoring flow charts use coded CGI transactions to evolve. These transactions take place from time to time (the rate can be adjusted with eTiceSoft), and impose a load on the network. Luckily, the transactions are optimised to keep the quantity of data exchanged - and hence the update time between two image refreshes - to the minimum.

So, the flow chart is first loaded in the navigator (which takes the longest depending on its size), and then refreshed from time to time.

By default, the TCP/IP port through which the http data is transmitted is port 80. But for various reasons (security, networking several MIIWebs behind a single gateway ...), it may be preferable to change this port number.

This can be achieved using MIIWeb's on-line configuration panel.

III.1.2 - Making the WEB Connection

There are two ways of connecting to an MIIWeb which is connected to a network :

a) Via the MIIWeb's IP Address

In the navigation window, in the URL entry field, type in the MIIWeb's IP address (accessible to or compatible with your network).

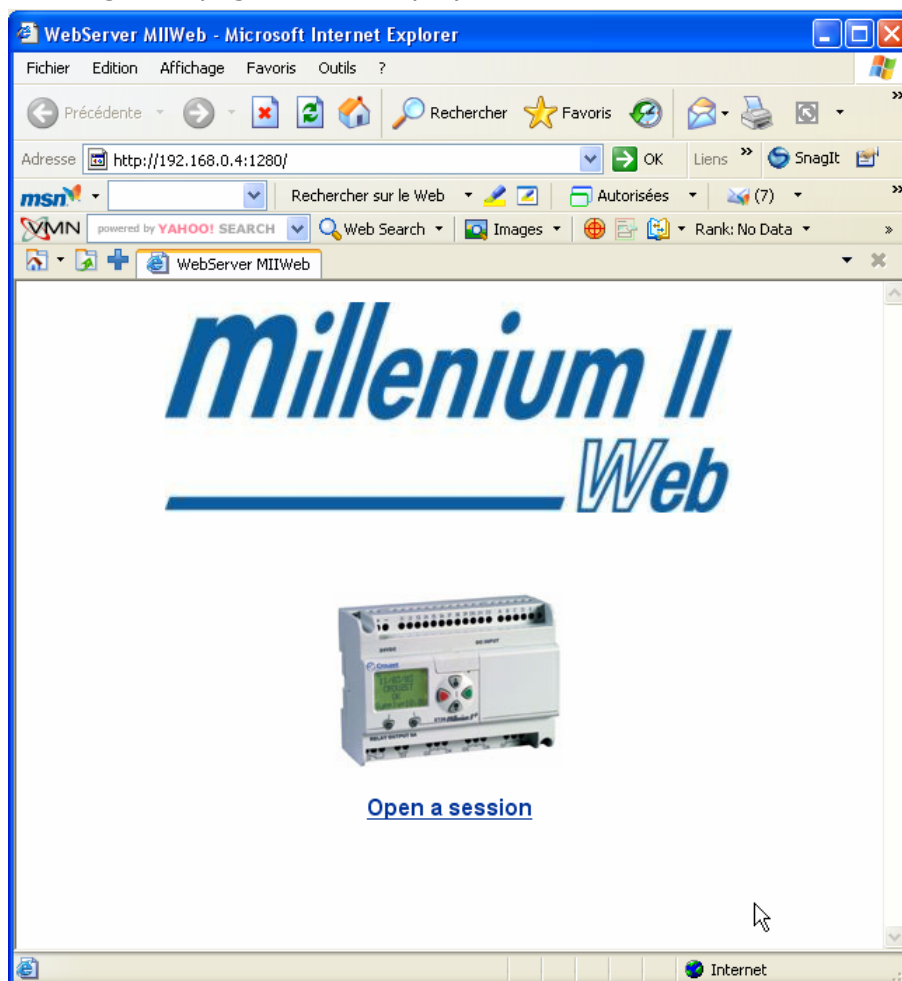
On leaving the factory, MIIWeb is pre-programmed with the following parameters:

IP Parameters	Value
IP address	192.168.0.4
Sub-network mask	255.255.255.0
Gateway	192.168.0.1
DHCP Client	Deactivated

Example:

Adresse  http://192.168.0.4/   OK


The following WEB page is then displayed:



b) Via an URL or Domain Name

In this case, the user has opened a DynDNS account or has registered his network's fixed IP address with a DNS server.

On condition that this DNS server is accessible from the LAN or WAN to which the MIIWeb is connected, then just enter the URL attributed to the remote MIIWeb associated with the corresponding IP address, in the URL field in the workstation's navigator.

Adresse  http://www.mymiiweb.com/   OK

Although it is more complex to set up, this is the easiest solution for the end user.

c) Comments :

- The IP address or the URL for consulting the MIIWeb must be accessible from the network in which the http client is located, either because the MIIWeb concerned belongs to the same sub-network, or because the gateway for the HTTP client's sub-network gives access to the network in which the MIIWeb is located.

- The port number on which the navigator will make the http connection can be specified in the URL, using the separator « : » :
<http://192.168.0.4:83> in this example, the MIIWeb is interrogated and must respond on TCP/IP port 83
<http://www.monmiiweb.com:546> in this second example, MIIWeb is interrogated and must respond on TCP/IP port 546.

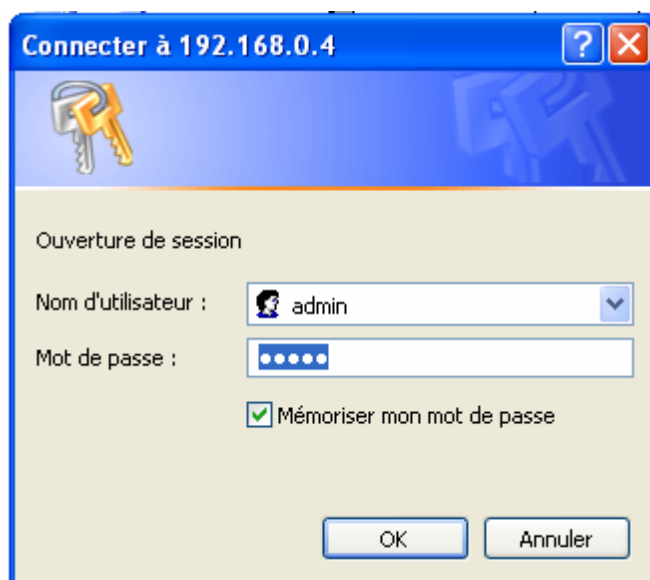
- It is imperative that the port number used be open to the network used; this may require configuring certain fire-walls or routers in the network installation.

III.1.3 - Starting a Session

a) Sessions

Once the navigator and the MIIWeb are connected, the TCP/IP-http frames can circulate properly. At this point, MIIWeb presents its home page. MIIWeb cannot be operated from this cover page, but access to the session manager is provided from it. This ensures a certain level of security for the MIIWeb and the installation it monitors.

After clicking on the « Start a Session » Hypertext link, the session manager displays an authentication window:



MIIWeb then requests the user session name and password to start a session.

MIIWeb's session manager manages 3 levels of responsibility, corresponding to three user session names.

Each category is associated with the right to access certain MIIWeb functions :

Session Type	Authorised Operations
Operator <u>Rights :</u> Minimum Factory Codes : LOGIN : user PASSWORD : user	Pages accessible and interaction authorised: <ul style="list-style-type: none"> - Remote maintenance - Monitoring (visualising states) without being able to change the state of the system - Archiving, without being able to delete the archive file

Supervisor <u>Rights</u> : Middle level Factory Codes: LOGIN : respo PASSWORD : respo	Pages accessible and interaction authorised: <ul style="list-style-type: none"> - IP configuration - Remote maintenance with the possibility of changing the state of the IXC words (writing) - Monitoring (visualising states) with the possibility of changing the state of the process monitored - Archiving, without being able to delete the archive file
Administrator <u>Rights</u> : Maximum Factory Codes: LOGIN : admin PASSWORD : admin	Pages accessible and interaction authorised: <ul style="list-style-type: none"> - IP configuration - Advanced configuration panel (activating services, password management ...) - Remote maintenance with the possibility of changing the state of the IX words (writing) - Monitoring (visualising states) with the possibility of changing the state of the process monitored - Archiving, including the possibility of deleting the archive file

b) Security, Limitations and Notification

For security reasons, MIIWeb only allows simultaneous access via http to 5 different client stations (with different IP addresses).

If a sixth client should connect, MIIWeb rejects the connection request and, if the person who attempted the connection is an administrator, displays the list of the various IP addresses already connected to the MIIWeb and having started a session.

Comments :

- The number of users connected at any given moment is shown in MIIWeb's Menu Bar (OnLine : x).
- The connection manager notifies every new connection attempt in MIIWeb's logbook, listing the date, time and IP address of the client station from which the attempt was made, and the number of connections open at that time.

	Remote Maintenance	Monitoring	Settings	Log	Archiving	2006/04/17
	OnLine : 1					22:16

Configuration panel

URL (DynDNS): m2webtest.dyndns.info

TCP/IP Settings - Ethernet

ID :	M2Web	IP Address :	192.168.0.4
MAC :	00-30-56-80-0E-29	Subnet Mask:	255.255.255.0
DHCP Client enabled :	<input type="checkbox"/>	Default gateway :	0.0.0.0
HTTP Port :	1280		

Reconfigure

PPP Status

PPP Client not available

III.2 - Menu Bar

As soon as a session is started, MIIWeb displays its **Menu Bar** and the first monitoring page (Page0).

This Menu Bar enables the user to select the pages he wishes to view using a navigation menu, but also shows information on the status of the system such as the current date and time, the number of people connected, the status of the alarms or again, the GSM network reception level (for on-board applications).

III.2.1 - The Navigation Menu

This is a series of hypertext links giving access to some of MIIWeb's display pages.

Although these links are displayed whatever the category of the session in progress, they are activated or deactivated according to the rights authorised by the session manager.

So, some pages remain inaccessible to some users, depending on the type of session they have started (Operator, Supervisor or Administrator).



III.2.2 - Connection Data

The connection data show the user the number of sessions in progress at that time, and the GSM network reception level, where a GPRS MODEM is used.

The number of sessions in progress enables the user to be aware that others may take control of the system. This means, for example, that an operator may view a state change in a monitoring flow chart, made by a supervisor or an administrator, while he himself is not able to change this state.

Several administrators or supervisors may send contradictory orders to the MIIWeb; although this may cause problems, it remains the users' responsibility.

The GSM signal reception level is represented in the form of a bar-graph indicating the quality of the network reception for the wireless telephone operator whose SIM card is activated in the GPRS MODEM.

When a client PPP connection is made to the GPRS network APN or PPP Server, MIIWeb is no longer able to refresh this data, which only represents the state of the quality of network reception at the moment the PPP connection was made.



III.2.3 - Date and Time

This field may display the time and date of the MIIWeb system, but also the last system alarm triggered.

Date format: Year/Month/Day

2006/04/17
21:53

MIIWeb has its own internal clock, however, this is not saved, so it is reinitialised every time power is applied or the system is re-started.

During the initialisation, MIIWeb synchronises its system time to the first Millenium in its registration list or to the selected PLC used for it. Then from time to time, it attempts to synchronise its system time with the same Millenium or PLC again.

Time synchronisation may be forced by clicking on the blue centre bar, which becomes green if no system alarm is triggered.

2006/04/17
21:53

If a system alarm is triggered, the centre bar becomes red and the alarm name is displayed below it:

2006/04/17
FAULT M2 #2

Here, a communication fault with the first Millenium on the list has been detected.

The date and time information is updated every minute.

When MIIWeb is in start-up and initialisation phase, the Waking Up alarm is active and symbolised by an orange centre bar, indicating that MIIWeb's availability is not optimal.

Le 00/00/0000
Waking up

III.3 - The Monitoring Page

III.3.1 - Selecting the Flow Chart

When an http connection is made or the user clicks on the « Monitoring » Hypertext link in the navigation menu, by default, MIIWeb displays the first monitoring page created with eTiceSoft.

Several animated flow charts can be created with the eTiceSoft software. They are identified by an HTM file (*.htm) on the MIIWeb's internal hard disk drive. One flow chart may call up another, since eTiceSoft is capable of creating automatic menus, or links between these pages that the user can change at will. These inter-page links are activated by simply clicking on the mouse, thus causing the appropriate flow chart to be displayed on the WEB monitoring page.

III.3.2 - Utilisation and Limits

A monitoring flow chart consists of objects with dynamic behaviour, which are regularly refreshed by CGI transactions between the HTTP client (Navigator) and the Server (remote MIIWeb).

These transactions use HTTP 1.0 so data security is not assumed by the WebServer itself but only by the Network strategies used around it.

The refresh rate for each object is specified using eTiceSoft, and may vary from 400ms to 4 seconds. If a flow chart contains several tens of objects, refreshing all the objects may take several seconds, or even several minutes. So where the priority is on the fluidity of the animation, a flow chart should have a limited number of objects.

The user can control the buttons and certain other objects with the mouse; positioning the mouse over one of these and pressing the right button gives that object priority, freezing all the other objects in the flow chart in their then-current state. For example, when a cursor is depressed for an extended period, the other objects are frozen for that period.

To optimise network transactions, the position of a user-modifiable object is only transmitted to MIIWeb after the button has been released.

Orders transmitted to MIIWeb are only taken into account at the end of each scan cycle. So a delay in the cycle caused by the absence of a response from a MODBUS slave for example, results in a delay in action from the monitor's point of view. This delay may last up to several seconds in the event of serious problems in communication with MIIWeb and with its environment.

Moreover, if the MODBUS slave or the Millenium concerned by the button being pressed has a connection fault with the MIIWeb, the order is cancelled or is simply not taken into account, which the monitoring flow chart cannot indicate to the user, unless flow chart designer has planned for such situations.

III.4 - The Remote Maintenance Page

This page provides for displaying all the XC/XN exchange words for a Millenium registered to MIIWeb. If communication with one of the MIIWebs is not reliable, MIIWeb indicates this, specifying each time a communication fault occurs, how the MIIWeb is connected and its address, where appropriate, on the MODBUS network (if it is not an adjacent connection).

It is possible to display the status of the 8 Milleniums devices which could be connected to the MIIWeb. The MIIWeb number is displayed at the top of the remote maintenance page.

It is possible to change Milleniums using the « Previous » and « Next » arrows to the left and right of the Millenium number.

If the user has started an « Supervisor » or « Administrator » session, he can force the state of the bits in IX exchange words by clicking on them. Of course, this is not possible for the OX exchange words, since they are only accessible for reading.

This forcing function can be very useful in testing the behaviour of a Millenium program monitored by an MIIWeb or to force a Millenium into a particular state provided for in its program.

If the user selects a Millenium which is not registered in the eTiceSoft registration table, MIIWeb displays the message « Does not exist » in the « Information » field.

< Previous
Millenium : 2
Next >

Status : Connected by MODBUS : Address: 3

Data of exchange in reading

XC Bits																	
	OXC 01	OXC 02	OXC 03	OXC 04	OXC 05	OXC 06	OXC 07	OXC 08									
XC Words	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Decimal
OXC 09	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
OXC 10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	1080
OXC 11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0

Data of exchange in writing

XC Bits																	
	IXC 01	IXC 02	IXC 03	IXC 04	IXC 05	IXC 06	IXC 07	IXC 08									
XC Words	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Decimal
IXC 09	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	1
IXC 10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	4
IXC 11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	17

The decimal field at the end of the OX and IX lines gives the value expressed in "base 10" of the content of the corresponding XC/XN word.

III.5 - The Configuration Pages

When the user has started an Administrator or Supervisor session, clicking once on the Configuration menu, displays the main configuration panel.

Comment:

MIIWeb only accepts alphanumeric characters as valid characters.

III.5.1 - The Configuration Panel

This panel provides for configuring all the IP parameters of the MIIWeb on line. It also provides for displaying the status of the client PPP or server connections or for attempting to make or cut off a connection if necessary.

This page is refreshed automatically every minute; this is why any changes must be made in this limited time interval.

If MIIWeb's DynDNS service is configured, the DynDNS domain name of the MIIWeb is displayed in bold typeface:

URL (DynDNS) : mydyndnsURLaddress.x



Configuration panel

URL (DynDNS): m2webtest.dyndns.info

TCP/IP Settings - Ethernet

ID :	M2Web	IP Address :	192.168.0.4
MAC :	00-30-56-80-0E-29	Subnet Mask:	255.255.255.0
DHCP Client enabled :	<input type="checkbox"/>	Default gateway :	0.0.0.0
HTTP Port :	1280		

[Reconfigure](#)

PPP Status

PPP Client not available

[Connect PPP Client](#)
[Disconnect from PPP Network](#)

Rebooting

[Reboot the WebServer](#)

Advanced configuration

Administrator only

a) Configuration of the TCP/IP - Ethernet Stack Zone

All the TCP/IP addressing parameters can be reconfigured from this zone.

ID: from a network and in particular from eTiceSoft, MIIWeb is identified by a ID. This name is shown in certain messages or alarms. By default, this identifier is: M2Web; it can be modified by the user. This field must not be more than 10 characters long.

MAC Address: This address is unique for each MIIWeb manufactured and provides unique identification world-wide for each unit. In fact, MIIWeb's serial number is extracted from the last 5 characters of the MAC address. It cannot be modified by the user and is displayed for information. This address is recorded in the archive files produced by MIIWeb.

DHCP Client enabled: This box activates or deactivates the MIIWeb's DHCP client. If this box is checked, it is imperative that MIIWeb be connected to a network with a DHCP server, which will immediately be interrogated by MIIWeb to obtain a new valid IP address.

If no DHCP server is present, the IP address 0.0.0.0, which is not valid on any network, will be allocated by default to the MIIWeb.

HTTP Port: this field provides for setting the TCP/IP port number to ensure http consultation (Internet Navigator). This port number is used by the MIIWeb Webserver. As soon as this port number changes, the http connection to the server is cut off, and no further pages may be refreshed until a new WEB connection is made on the appropriate port. This port number is used and is common to all users wishing to connect to MIIWeb via the WEB.

It is IMPERATIVE that this field contains a decimal value (in base 10) between 1 and 65530.

IP Address: This field provides for modifying MIIWeb's current IP address. If this changes, any ongoing communication with the MIIWeb is cut off for all clients who were connected at that moment.

E.g.: 192.168.0.4

WARNING ! The IP address entered in this field must have the format w.x.y.z where w, x, y and z represent a decimal number between 0 and 255.

Sub-network Mask: this field provides for modifying MIIWeb's sub-network mask.

WARNING ! This mask must be in the same format as the IP address (4 decimal numbers between 0 and 255 and separated by a dot).

E.g.: 255.255.0.0

Gateway: This field contains the address of the gateway or of the router for the sub-network to which MIIWeb is connected. This address is in the same format as the IP address (4 decimal numbers between 0 and 255 and separated by a dot).

E.g. : 192.168.0.1

Comment: if the format is wrong in any of the above fields, a system error may occur, and only the eTiceSoft software and its downloading manager can reconfigure MIIWeb properly.

For MIIWeb to take account of any changes, click on the « **Reconfigure** » button. This operation may take several minutes.

b) Status of the PPP MODEM Connection Zone

This zone provides for displaying the status of the PPP connection via the GPRS MODEM or STN MODEM.

Status: This line shows the status of the current PPP connection.

The various statuses possible are as follows :

Status Displayed	Meaning
Status: Connected:IP : x -Server Provider:y -DNS1:z -DNS2:w	A client PPP connection has been made with the Provider or the APN, MIIWeb's IP address is shown, as is the server's. If DNS servers are accessible, their respective addresses are shown. This connection prevents any simultaneous connection to MIIWeb's PPP server.

Status: Connected temporarily to send an eMail : PPP IP address : x Provider's server IP address : y	A client PPP connection has been made to the Provider or the APN, MIIWeb's IP address is shown, as is the server's. Here, this connection has only been made to send an eMail. This connection prevents any simultaneous connection to MIIWeb's PPP server.
Status: Disconnected	No PPP connection is active at this time. But the PPP client is operational.
Status : Unable to connect	The PPP client is not operational (MODEM initialisation error)
Status: Client PPP connection attempt in progress ..	A client PPP connection is in progress. This operation may take several minutes.
Status: Disconnection from the PPP server in process ...	Disconnection from the PPP server is in progress, MIIWeb performs all the MODEM steps necessary. This operation may take several minutes.
Status : No client PPP connection active	The PPP connection parameters are incomplete or an error connecting to the MODEM has occurred.
Status: PPP Server session in progress : IP=x, IP Client=y	A remote PPP client has connected to MIIWeb's PPP server. This incoming connection prevents the PPP client from connecting.

Program: MIIWeb can connect automatically or from time to time to a Provider's PPP server via an APN (GPRS). In this case, it follows a connection program prepared using the eTiceSoft software workshop. This program is displayed in the corresponding information field and the text displayed may be :

Program Information Text	Meaning
Program : Request for Permanent connection	Means that MIIWeb continually attempts to connect to a PPP client. This connection can only be achieved if MIIWeb has effectively detected a MODEM and succeeded in initialising it. This program prevents connection to MIIWeb's PPP server. The attempt to make a PPP client connection is repeated at regular intervals (approx. 5 minutes).
Program : Attempt to connect at start_time - Disconnection at end_time	Means that the MIIWeb is in the Intermittent connection mode. It systematically attempts to connect during the period from start_time to end_time. During this period, MIIWeb attempts to make the connection every 5 minutes if the PPP client connection is not active. An attempt to connect to the Provider's PPP server automatically occurs if MIIWeb needs to send an eMail.
Programme : automatic client PPP connection deactivated	Means that MIIWeb has deactivated its automatic connection program, because a user has forced connection or disconnection from the configuration panel.

The « **Connect now** » button: This button forces MIIWeb to connect to the Provider's PPP server. This priority action must be used prudently, but is very useful for checking that the MODEM parameters are correct. This action deactivates the automatic connection mode. The only way to reactivate the automatic mode is to press MIIWeb's « Disconnect » button.

The « **Disconnect** » button: This button forces the PPP client to disconnect from the Provider's PPP server. This reactivates the automatic connection mode, which then recovers the normal operating mode specified using eTiceSoft.

Le bouton « **Activate program** » : This button reactivate the PPP Client connection program defined with eTiceSoft in the project loaded in the WebServer after a manual Connection or Disconnection.

c) Re-boot the WebServer

This button forces the WebServer to re-boot to take new parameters into account immediately; it should not normally need to be used except during optimisation phases.

III.5.2 - Advanced Configuration of the WebServer

This panel is only accessible to MIIWeb's administrator; it provides for configuring MIIWeb's internal parameters, such as session codes, MODEM codes, for activating or deactivating certain network services, for resetting the time on the system clock and on the Milleniums connected...

This page is refreshed every minute. So any change to any of the parameters and the reconfiguration must be completed within this time frame, or the change will be cancelled and the field returns to its initial state.

a) Configuring the Network Services

This zone provides for activating or deactivating MIIWeb's network services.

Parameter setting of the network services			
<input checked="" type="checkbox"/> DNS		<input checked="" type="checkbox"/> SMTP Client (Mails)	
Primary DNS IP :	<input type="text" value="0.0.0.0"/>	SMTP Server :	<input type="text" value="smtp.orange.fr"/>
Secondary DNS IP :	<input type="text" value="0.0.0.0"/>	Server IP Address :	<input type="text" value="193.252.23.129"/>
<input type="button" value="Reconfigure"/>			
<input checked="" type="checkbox"/> TELNET		<input checked="" type="checkbox"/> FTP	
Login :	<input type="text" value="tel"/>	Login :	<input type="text" value="ftp1"/>
Password :	<input type="text" value="tel"/>	Password :	<input type="text" value="ftp1"/>
Telnet TCP - PORT:	<input type="text" value="23"/>	FTP TCP - PORT:	<input type="text" value="1221"/>
<input type="button" value="Reconfigure"/>			

DNS:

This service enables MIIWeb to interrogate the Primary DNS servers or if not available the Secondary DNS service, to obtain the IP address of a server from its domain name. This service is useful in particular to access the SMPT message Server if the DynDNS server does not know its IP address.

The DNS box provides for activating the service (box checked) or deactivating it (box not checked).

It is imperative that the DNS servers' IP addresses be known and entered in the right format in the reserved fields when configuring manually.
(4 decimal numbers between 0 and 255 and separated by a dot).

When configuring via the DHCP client, and as long as it is correctly configured and has the appropriate function, the Primary and Secondary DNS servers can be detected automatically. However, manual configuration remains the most reliable.
The DNS service operates on TCP/IP port **53**.

SMTP Client (for eMails):

This service can be deactivated by not checking the « SMTP Client (for eMails) » box. If this client is deactivated, no eMail can be sent.

If the address of the SMTP client is unknown, it is possible, if the DNS services are operational, to use this server's domain name to access it. In this case, and if the name resolution is successful (DNS accessible), then the SMTP server's IP address is automatically detected and updated (value displayed in the corresponding field). If the name resolution fails (DNS overloaded or not available), an error message is marked in the log. This field may not be more than 68 characters long.

The « **SMTP server's IP Address** » field provides for configuring this server's IP address manually. Where domain name resolution is successful (DNS active and domain name valid), this field is automatically filled in by MIIWeb with the current address of the SMTP server provided by the DNS servers.

Before sending an eMail, MIIWeb attempts to resolve the SMTP server's domain name, in order to obtain the SMTP server's latest address (very useful for Ethernet/GPRS MODEM switching).

The SMTP service operates on TCP/IP port **25**.

TELNET:

This service is very useful for diagnosing MIIWeb, and displays MIIWeb's on-going operations in text form. This service can be deactivated, hence prohibiting the use of MIIWeb's diagnostic mode. Any attempt to make a TELNET connection will then be rejected. The service is deactivated if the TELNET box is not checked.

When a TELNET session is started by a client, it starts with an authentication phase

Username: provides for identifying the user. This field must not be more than 10 characters long.
By default, this field contains the value « tel ».

Password: provides for authenticating the session.
This field must not be more than 10 characters long.
By default, this field contains the value « tel »

```

Telnet 192.168.0.4

M2Web Telnet session
Username: tel
Password: **
Unknown user or password
Username: tel
Password: ***
User logged in

MODBUS time out !
MODBUS : Received 0 bytes
MODBUS : Received 5 bytes
MODBUS : Received 5 bytes
MODBUS : Received 5 bytes
MODBUS : Received 5 bytes
MODBUS : Received 5 bytes
MODBUS : Received 5 bytes
MODBUS : Received 5 bytes
MODBUS : Slave 5->6=0009
MODBUS time out !
MODBUS : Received 0 bytes
    
```

After three successive unsuccessful connection attempts, MIIWeb closes down the TELNET client.

The TELNET server's port number incorporated in MIIWeb can be changed, this port number is entered in the « TELNET Port » field; by default the Telnet port is 23. The port number must be a decimal number between 1 and 65535. it is imperative that this value be entered in numeric form (base 10).
E.g. : 897

Comment:

After loading eTiceSoft projects using a MODEM, the TELNET parameters are reinitialised to their default values.
So the MIIWeb administrator has to configure the TELNET service again.

Only one single TELNET session may be in progress at any given moment.

FTP Service:

This service enables a standard FTP client to connect to MIIWeb to download files. This service is used by eTiceSoft to download the files compiled for a project into the MIIWeb (with specific priority authentication codes).
The FTP client (just like the TELNET client) must use a specific TCP/IP **port** to make a connection with the FTP server. This port number is set by default to 21 (standard port for FTP servers). This port number can be modified by changing the content of the « **FTP Port** » field. The port value is a decimal number (expressed in base 10) between 1 and 65535.
E.g.: 675

An FTP session starts systematically with an authentication phase.
The FTP server verifies the Username and the associated Password.
The Username and password can be changed by entering new data in the corresponding fields :

Username: this field shows the current Username for the session requested by the FTP server on making the connection. The value in this field must not be more than 15 characters long.

Default value : ftp1

Password: this field shows the current password for the session requested by the FTP server on making the connection. The value in this field must not be more than 15 characters long.

Default value : ftp1

Activation/deactivation of the FTP service: a key for security

This service can be deactivated by unchecking the FTP box: this means that the MIIWeb FTP server can then no longer be accessed. MIIWeb's entire file system is then protected against all attacks from the outside.

But in this case, it is also impossible to load a new project using eTiceSoft. Deactivating this service represents a simple and effective means of protecting the data in the MIIWeb.

When the user connects to the FTP server, if he starts a session using the codes above, MIIWeb automatically directs him to the archive directory on his hard disk drive.
The following files are placed in this directory (if they exist) :
Archive.txt : archive text file containing the data archived by MIIWeb's event manager.
Logfile.txt : text file containing MIIWeb's logbook records.

Comment:

After loading eTiceSoft projects using a MODEM, the FTP parameters are reinitialised to their default values.

So the MIIWeb administrator has to configure the FTP service again.

Only one single FTP session may be in progress at any given moment.

Activating the Reconfiguration:

After changing the desired parameters, the service is reconfigured on pressing the « **Reconfigure** » button. Reconfiguration may cause the MIIWeb to re-boot, which may take several minutes.

Dynamic DNS Client (DynDNS):

<input checked="" type="checkbox"/> Dynamic DNS Client (DynDNS)	
DynDNS Server URL:	members.dyndns.org/nic/update
Login :	tddp
IP to be refreshed :	
Password :	trontp
Domain name to update :	m2webtest.dyndns.info
<input type="button" value="Reconfigure"/>	

The DynDNS client provides for accessing a service with a dynamic domain name to record an IP address which may have changed. This service is very useful should a dynamic IP address be allocated to MIIWeb by the Internet network.

This service can only operate if MIIWeb's DNS service is operational (DNS servers' IP address suitable and servers accessible from the LAN or WAN where MIIWeb is installed).

Server's URL: this field provides MIIWeb with the URL DynDNS service Provider it must contact to register MIIWeb's new information (new IP address).

In most cases, the DynDNS entity (www.dyndns.org) provides this service, in which case this field's value is « **members.dyndns.org/nic/update** ».

Each time a DynDNS refresh attempt is made, MIIWeb calls the DNS service, if the request fails, the DynDNS service cannot be updated, and this is consigned in the log book. This field may not be more than 99 characters long.

IP Address to be refreshed: This field contains the current IP address which has effectively been refreshed by the DynDNS client, if this field is empty, no address has been sent to the DynDNS service. The address which is refreshed by default is MIIWeb's current IP address.

If a PPP connection is ongoing, MIIWeb's current address is the address used for the PPP connection. If no PPP connection is in progress, the MIIWeb uses its Ethernet address as the current address. This field may not be more than 16 characters long. The IP address must be entered in the right format (4 decimal numbers between 0 and 255 and separated by a dot).

Login: Connection to the DynDNS service starts with an authentication phase. When taking out a DynDNS subscription, the user specifies a session name, this session name is used to authenticate the DynDNS connection. This session name is shown and can be modified via this field. The field may not be more than 20 characters long.

Password: Like the session name, the password is specified on subscribing to the DynDNS service. This field provides for entering or viewing it. The field may not be more than 20 characters long.

Domain Name to update: When taking out a DynDNS service subscription, the user chooses a domain name (or URL) to identify his device. This domain name must correspond to the current IP address of the device to which the user wishes to connect, in this case, MIIWeb's IP address as seen from the Internet. This field may not be more than 70 characters long.

DynDNS service reconfiguration is only effective after pressing the « **Reconfigure** » button.

The TCP/IP port used for the DynDNS service is port 80.

b) Modifying the Identification Codes

For MIIWeb, a user has rights. These rights are specified by the session manager. The session manager manages three levels of responsibility (or rights). These rights are assigned on starting the WEB session. A session is started once a suitable Username and password have been entered by the user and as long as the number of sessions in progress is below the maximum allowed.

There is a different session name and password for each category. The fields in this zone of the advanced configuration panel provide for specifying the available responsibility level session codes. Each field may not be more than 15 characters long.

User's session codes	
Operator	Supervisor
Login : <input type="text" value="user"/>	Login : <input type="text" value="respo"/>
Password : <input type="text" value="user"/>	Password : <input type="text" value="respo"/>
Administrator	
Login : <input type="text" value="admin"/>	
Password : <input type="text" value="admin"/>	
<input type="button" value="Reconfigure"/>	

The session codes are only effectively updated by pressing the « **Reconfigure** » button.

As soon as a new session code is specified for the current session, MIIWeb requests the user to enter it to continue WEB navigation.

c) Setting the Time on the MIIWeb and Milleniums Connected

MIIWeb has its own system clock. However, from time to time (around every 5 minutes), MIIWeb attempts to synchronise it with the real-time clock stored in the first Millenium II registered using the eTiceSoft software workshop. Each time MIIWeb is re-booted, the time and date are reinitialised.

From this zone of the advanced configuration panel, at one go, it is possible to reset the time on MIIWeb's system clock, but also that of all the Millenium II devices registered to MIIWeb in the eTiceSoft project currently in progress.

SYSTEM			
Date and time			
Hours :	<input type="text" value="22"/>	Minutes	<input type="text" value="25"/>
Day :	<input type="text" value="17"/>	Month :	<input type="text" value="4"/>
		Year :	<input type="text" value="2006"/>
<input type="button" value="Reconfigure"/>			

From this panel, the time specified using the « Hour » and « Minute » fields, and the date specified using the « Day », « Month » and « Year » fields can be updated on pressing the « **Reconfigure** » button.

The **Hour** field is a decimal number between 0 and 23.

The **Minutes** field is a decimal number between 0 and 59.

The **Day** field is a decimal number between 1 and 31

The **Month** field is a decimal number between 1 and 12,

The **Year** field is a decimal number between 2000 and 2099.

When the « **Reconfigure** » button is pressed, a Timeset command is sent to all the Millenium II devices connected to and registered with an MIIWeb.

d) MODEM Initialisation and Client PPP Connection Parameters

MODEM initialization and PPP Client settings	
<input checked="" type="checkbox"/> MODEM	
PIN Code of SIM card :	<input type="text" value="0000"/>
PUK Code :	<input type="text"/>
Modem Status: MODEM not found	
<input type="button" value="Reconfigure"/>	
PPP Client settings	
Provider phone number :	<input type="text" value="*99*1#"/>
LOGIN :	<input type="text" value="orange"/>
PASSWORD :	<input type="text" value="orange"/>
<input type="button" value="Reconfigure"/>	

This zone provides for displaying the MODEM status and for setting the SIM card initialisation parameters where a GPRS MODEM is used.

The MODEM has been detected and synchronised if the « **MODEM GSM / GPRS** » box is checked.

The **SIM card PIN code** field is only of use when a GPRS MODEM is used; it provides MIIWeb with the PIN code number of the SIM card it must use to initialise it. This field accepts a decimal number no more than 6 figures long (usually 4 figures) representing the PIN code of the SIM card used.

WARNING ! The PIN code must be valid from the moment the MIIWeb connected to a powered GPRS MODEM is itself powered up. Otherwise, MIIWeb will attempt to initialise the MODEM and the SIM card with a wrong code, which may cause the card to lock up and oblige the user to contact his SIM card supplier to obtain the PUK code to unlock it. RECOMMENDATION: do not power up a GPRS MODEM without having checked beforehand that the PIN code in the MIIWeb is the right one.

Should the SIM card lock up, the user can fill in the **PUK Code** field with the code provided by SIM card supplier to unlock the SIM card which has been locked up by a PIN code error.

The **MODEM State** field shows the state which the MODEM is in as a result of the AT commands sent by the MIIWeb to the MODEM connected to it.

If a GPRS MODEM is in use, and if the initialisation has been completed correctly, this field shows the reception level of the GSM signal. This information is also used to display the GSM network bar-graph in the navigation menu.

If the initialisation phase failed, MIIWeb displays « **MODEM Error** » in this field.

If the MODEM connected is an STN MODEM, MIIWeb displays « **MODEM OK** » in this field.

The PPP client parameters provide for specifying on line :

The Tel No. of the Provider's Server: This number is dialled by the MODEM to access the Provider's server. Where a GPRS MODEM is used, it is mandatory that this telephone number be the code for calling the APN : *99***1#.

This field may not have more than 16 alpha-numeric characters with the following particularities :

If the first character entered is a space, it is automatically replaced by the « + » sign, symbolising an international number.

If the last character entered in this field is the letter « d », MIIWeb replaces this character by the symbol « # », used to represent the APN code : *99***1# which will be entered as : *99***1d

The **character # is prohibited**, as are all non alpha-numeric characters, since their use may result in erroneous interpretation of the parameters transmitted to MIIWeb.

Username (LOGIN): when making a PPP client connection, very often, a PPP authentication phase may be necessary. The authentication type depends on the PPP protocol used : PAP or CHAP, this is specified by the Provider. (In general, a link with an APN uses the PAP protocol, while a link with a Provider uses CHAP). This field may not be more than 18 characters long.

User Password: when starting a client PPP session, this password provides for authenticating the session from the PPP server's point of view. This password may not be more than 18 characters long.

e) Re-booting the WebServer

This button provides for re-booting MIIWeb, this may be necessary after an manipulation error or to reinitialise a MODEM which has just been connected without being initialised.

The re-boot may take several minutes.

III.6 - The Logbook

Clicking on the « Log » menu causes MIIWeb to display the logbook. This log only displays the 20 most recent events. To access older events, the logfile.txt file has to be downloaded, if this option has been provided for by the project designer.

The events are listed in English.

History of the 20 last events					
Date	Time	Event	System status	Info	Session
04/17/2006	22:16	FAULT	Cannot get SMTP Server IP Address by DNS smtp.orange.fr	193.252.23.129	-
04/17/2006	22:15	SMS FAULT	Could not send SMS : test M2WEB SMS 0	+33673480707	-
04/17/2006	22:15	SMS FAULT	Could not send SMS : test M2WEB SMS 1	+33673480707	-
04/17/2006	22:15	SMS FAULT	Could not send SMS : test M2WEB SMS 0	+33673480707	-
04/17/2006	22:14	SMS FAULT	Could not send SMS : test M2WEB SMS 1	+33673480707	-
04/17/2006	22:14	FAULT	Cannot get SMTP Server IP Address by DNS smtp.orange.fr	193.252.23.129	-
04/17/2006	22:13	SMS FAULT	Could not send SMS : test M2WEB SMS 1	+33673480707	-
04/17/2006	22:13	SMS FAULT	Could not send SMS : test M2WEB SMS 0	+33673480707	-
04/17/2006	22:13	SMS FAULT	Could not send SMS : test M2WEB SMS 1	+33673480707	-
04/17/2006	22:10	FAULT	Cannot get SMTP Server IP Address by DNS smtp.orange.fr	193.252.23.129	-

The logbook is presented in the form of a table.

The table contains several columns:

Date: Shows the date, according to MIIWeb's system clock, on which the Logbook event occurred. The date format is Day/Month/Year.

Time: Shows the time according to MIIWeb's system clock, at which the Logbook event occurred. The time format is Hour : Minute : Seconds.

Event: Shows the type or system task (MIIWeb) which caused the event. Where a fault is the cause this is indicated.

System Status: Specifies the type of event or what caused it.

Info: Shows any additional information on the event. It often specifies the status of the service where the event originated after the event's occurrence.

Session: May show the type of session which caused the event or the Username of that session. If MIIWeb's task management system is the cause of the Logbook event or detected it, the word SYSTEM may be shown in this field. The symbol " - " means that the event was detected during an initialisation phase or during one of MIIWeb's periodic tasks.

III.7 - The Archiving Page

This page displays the values of the states monitored by MIIWeb's event manager.

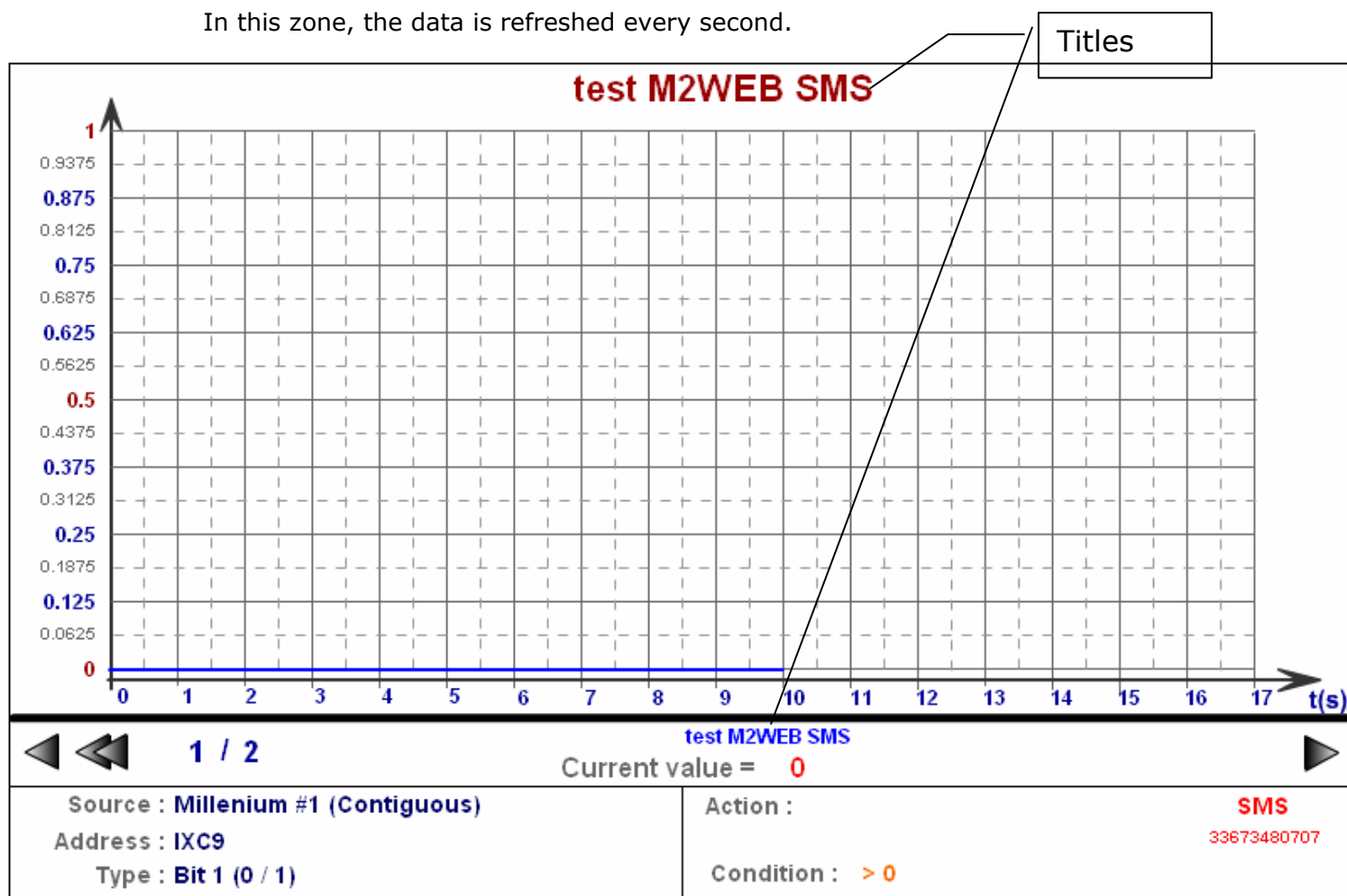
The page consists of two zones:

- the graph zone
- The disk space measurement zone.

III.7.1 - The Graph Zone

A graph provides for displaying « on line » the state and current value of each state monitored.

In this zone, the data is refreshed every second.



A graph is drawn, with a blue line. Drawing starts as soon as a valid value is sent by the MIIWeb.

The graph is reinitialised each time a new event is selected. It has automatic scaling.

An event can be selected by clicking on the arrows provided:



Two **Title** text fields placed respectively above and below the graph display the text associated with the state monitored by the event. This text depends on the action associated with the event.

The lower left field shows the **event number** and the **total number of events** defined using the eTiceSoft software workshop.

3 / 7

In this example, the user can observe the change in the state associated with event 3, in a project containing 7 events in all.

The **Current value** field represents the decimal value of the variable associated with the state of the event. In the case of a bit, the value of this variable may take one of two states : 0 or 2^(Binary weight of the bit concerned).

Below this, is a zone describing the event :

Source : this field specifies the origin of the state associated with the event, the communication bus through which MIIWeb accesses the state, and sometimes the MODBUS address of the slave where the state was detected.

Address : Specifies the address of the word in the MODBUS slave which is used to detect the state. This value is a decimal number (hence the presence of the lower case "d" at the end of the number).

Type : Specifies whether the state monitored is a 16-bit word (decimal value with a sign) or a bit. In this latter case, the binary weight of the bit is specified.

Action : Specifies the type of action performed by MIIWeb should the case or condition of the event be verified.

4 cases are possible and are displayed in full, the titles may vary according to the type of action.

Action	Title Texts	Description
Used by monitoring interface	Monitoring variable	eTiceSoft creates this variable when the behaviour of an animated flow chart object is associated with a variable whose source is not a Millenium
Archiving	Descriptive text (unit), defined using eTiceSoft	When the action is triggered, the data is filed in the archive file: archive.txt
eMail	Text of the eMail defined using eTiceSoft	When the action is triggered, MIIWeb attempts to send an eMail to the addressee whose address is shown in full.

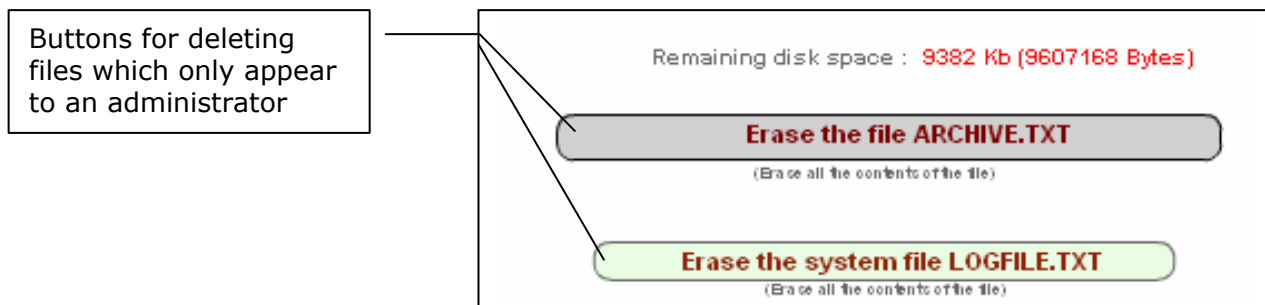
SMS	Text of the SMS defined using eTiceSoft	When the action is triggered and a GPRS MODEM fitted with an operational SIM card is connected, MIIWeb attempts to send an SMS to the addressee whose telephone number is displayed.
MODBUS redirection	The system code for the destination variable. This code is displayed for information and does not represent useful information, but if it is not shown, redirection is not possible.	When the action is triggered, MIIWeb recopies the value of the MODBUS word specified into another MODBUS slave at a different address. To display the destination word, refer to the eTiceSoft project.

Condition : specifies the condition under which the action is triggered. The trigger rules are specified in the Events chapter.

III.7.2 - The Disk Space Measurement Zone

This zone shows the user how much disk space is used by the various files in the archive directory, as well as the total remaining disk space.

If the user has started an administrator session, some additional buttons are at his disposal, enabling him to delete these files directly from the Internet navigator (this last operation is also possible via eTiceSoft's downloading manager with the administrator session codes).



Comments:

- The projects compiled by eTiceSoft are stored on the same disk as the archive files. Consequently, the bigger the flow chart files used by a project are, the less space is available for the archive files. So some transfer operations on projects compiled by eTiceSoft may fail, through lack of available disk space. The recommendation is to download then delete the archive files before transferring a project using big flow chart files.
- Th bigger a file is, the longer it takes to download it; while this is not a problem for LAN or WAN xDSL or Ethernet networks, it is much more of a penalty when transmitting data via GPRS or STN MODEM.

This measurement zone is refreshed once every minute.

IV - Events

MIIWeb can monitor the status of a system; to do so, it interrogates in a cyclic manner a certain number of devices connected to it in various ways. MIIWeb uses the concept of an event to perform this monitoring.

IV.1 - Definition

An event can be defined as a combination of the following elements:

- **A state monitored:** MIIWeb interrogates a specific data item in a device connected to it via MODBUS or via the adjacent extension. (on MODBUS, this may be a Millenium word or bit, or a 16-bit word contained in any RTU MODBUS peripheral)
- **A condition:** which, when met, triggers the action specified by the event. (this may be a state condition or a periodic condition)
- **An action :** this is the operation which MIIWeb is to perform when the condition is met (e.g. : archive the state, send an email or an SMS, or forward the value of the state monitored to another MODBUS peripheral)

Events are created either directly by the user, using the eTiceSoft software workshop, to archive, send an eMail or an SMS, re-copy a MODBUS word or by the graphics compiler which detects that an object situated on a flow chart depends on a state which is not already monitored by an event.

IV.2 - Limitations

MIIWeb has a maximum processing capacity of 100 events.

The conditions specified for events are tested at regular intervals (once per second).

The peripherals which contain a word or a bit subject to a monitored state specified in an event are interrogated from time to time by MIIWeb.

Since some of them may be connected on MIIWeb's RTU MODBUS interface, the scan time depends basically on the communication parameters specified on the RTU MODBUS network and on the number of slaves to be interrogated.

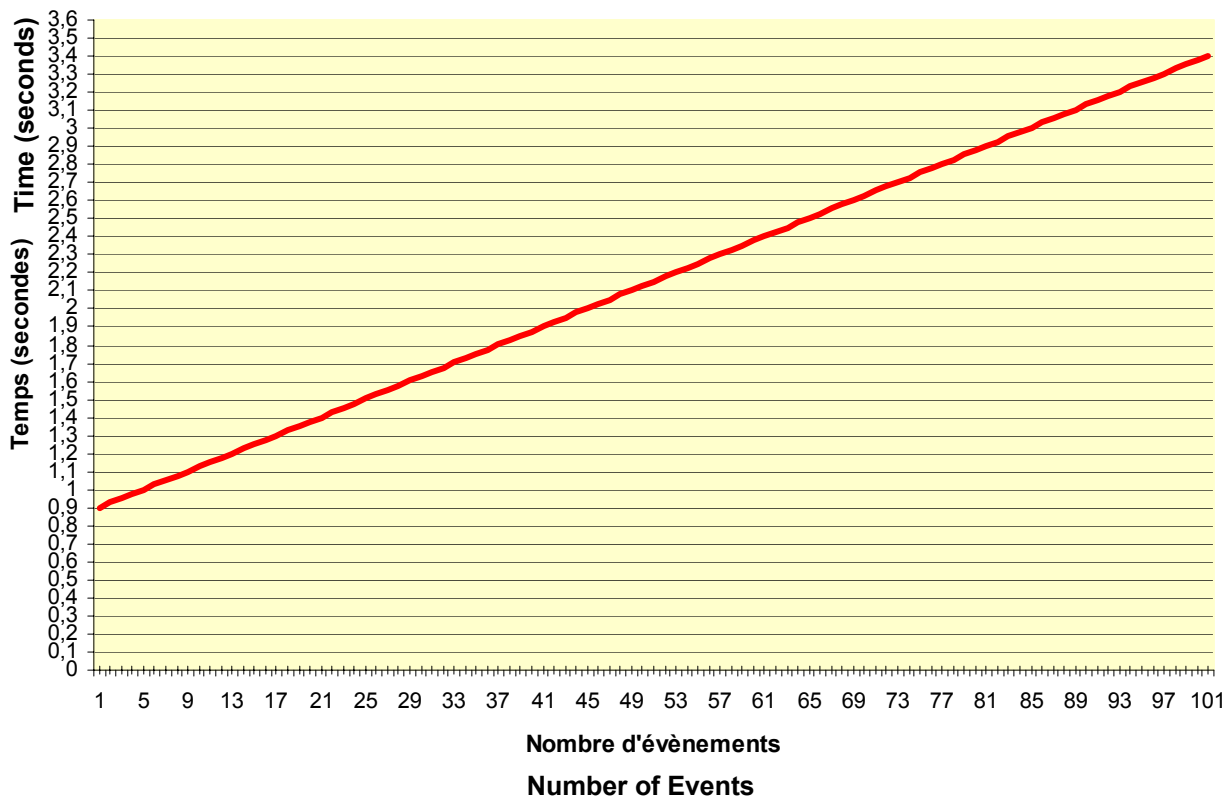
So the scan time for a state monitored is directly proportional to the number of events to be processed, and to the communication time for each of them.

Consequently, a state whose lifetime is shorter than the scan time for all the events cannot be detected.

This transitory state whose lifetime is shorter than the scan time is considered to be a parasite.

Theoretical evolution of the scan time as a function of the number of events (Conditions: all the event states are transmitted on a MODBUS communication at 19200 bauds with no faults and each event causes an archive record (disk access))

MIIWeb scan time as a function of the number of events (States monitored via RTU MODBUS at 19200 bauds) with no communication fault



IV.3 - Progress of a Scan Cycle: Critical Case

MIIWeb performs the following operations at every scan cycle:

Cycle Start

Read all the Milleniums registered:

- If one of the Milleniums has a problem, then a new read request is issued, extending the scan time.
- If the same Millenium poses a problem at the second attempt to access it, a fault is notified.

Read all the states of the events registered:

- If one of the states is not accessible, MIIWeb repeats its attempt to read it, extending the scan time.
- If the state still cannot be read, it is quarantined and will be re-interrogated 100 cycles later, to check the state of the connection again.

Cycle End

Each time there is no response to a read request; MIIWeb waits for the time specified by the MODBUS standard to send the next frame, this time can be as long as 1.5 seconds per read fault.

In the worst case, scanning 100 events and 8 Milleniums for faults may take around **350 seconds**.

A scan time of this length, resulting from the time constraints imposed by the MODBUS standard, makes the monitoring system unusable. So a fault has to be repaired as fast as possible or the project recompiled if a MODBUS slave monitored by an MIIWeb event is removed from the network.

IV.4 - Condition for Triggering the Action for an Event

An event contains an action which is triggered when the event condition is met.

Here is a simplified event processing algorithm:

- The state of an event is verified and compared cyclically against the value of the trigger condition, by an independent task in the scan cycle.
- The rate at which the trigger conditions are tested is 500 ms.
- When the trigger condition is met, the event is notified as activated.
- A third task, called the Event Manager is responsible for performing the actions for the events activated.
- When the Event Manager detects that an event is activated, then it performs the corresponding action (this action may take several minutes).
- When the action is finished, the Manager registers the event that it has just processed as completed and processes the next event activated.
- From that point on, the event will remain marked as completed as long as the event trigger condition remains true.
- Where an event is periodic, once the event action is completed, a time counter is reinitialised.

This system provides for processing events in the order of appearance and avoiding repeat processing (queue management).

However, processing event action is not done in parallel, so processing delays occur and in particular will accumulate. The action that takes the longest time is certainly action involving sending an eMail or an SMS, since these require synchronisation or connection to a service outside the MIIWeb and whose duration cannot be controlled to any great extent if at all.

V - Description and Technical Characteristics

V.1 - Hardware Aspects

V.1.1 - Connection

Utilisation	Connection
Power supply	2-stud screw terminal block for 1.5mm ² cables
Ethernet 10/100 Base TX with auto negotiation	RJ45 Female
RS232 connection for MODEM	DB9 Male
RS485 - MODBUS	3-stud screw terminal block for 1.5mm ² cables
Adjacent Millenium connection	16-pin terminal strip

V.1.2 - General Characteristics

Characteristics	Operating Range
Compatible Milleniums	Millenium II+ XT 20 -24V DC
Temperature	-5°C to +55°C
Power supply voltage	+15V to +24V DC +/- 10%
Dimensions	WxLxH : 72 x 90 x 60 mm
Maximum power absorbed	7 VA
Maximum inrush current	400 mA (10ms)
Storage capacity Maximum standard (for operating web pages + archive file)	30 Mega bytes on a COMPACT FLASH® board certified by Mecacel (8-bit bus compatible)
Maximum number of read / write cycles on integrated storage units	10000
Maximum initialisation time after each re-boot or each power up	2 minutes (including the MODEM search and synchronisation time)
Ethernet connection status indicator – Network traffic	Red LED on front panel
Status indicator : accessing storage unit	Green LED
Status indicator : communication with adjacent Millenium	Red LED
Voltage present indicator	Green LED
RS232 signals available	RTS, CTS, RXD, TXD, 0V
RS232 signal voltage levels	+/- 8V (+/- 20%)
Types of MODEMS compatible	See. list in eTiceSoft
RS485 line termination impedance	Integrated and always connected (resistor:120 Ohms +/-10%, 0.125 watts)
RS485 protection	No opto-isolation, but protected against surges <100V for 100µs
Maximum number of events	100
Maximum number of Milleniums connected	1 adjacent + 7 connected to RTU MODBUS on the RS-485 terminal block

Format of the archive file	Text file in the Tab tab return format, Records dated.
Access to the archive file	Downloaded using an FTP client or eTiceSoft
Network services active with Ethernet 100 Base TX connection	TELNET, FTP, http, UDP configuration server, DNS, DHCP, SMTP, DynDNS
Services accessible with a MODEM connection (Peer-to-Peer (PPP))	TELNET, FTP, http, SMTP, DynDNS

V.2 - Communication Characteristics

V.2.1 - Network Services (using TCP /IP)

V.2.1.1 WEB Server: TCP/IP http 1.0

Role: This server provides access to the monitoring functions offered by MIIWeb from an ordinary Internet navigator compatible with the Flash Player© plug-in by MACROMEDIA® which must be installed on the client machine.

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	YES if the PPP provider offers this service
Maximum number of simultaneous connections	3 with a refresh rate of every 2 seconds (on 100 Base TX network). Up to 50 simultaneous connections on 100 Base TX network with a refresh rate of 100 seconds.
Session authentication	Session Code and related Password (these codes can be managed by cookies); can be changed by the Administrator
Characteristics of the client software	Any navigator compatible with FLASH Player®© by Macromedia© which must also be installed on the client machine
TCP/IP port number	80 by default, can be changed by the Supervisor or Administrator
Deactivation by the administrator	NO
User sessions and rights	3 Levels : Administrator Supervisor Operator

V.2.1.2 FTP Server

Role: This server provides for updating the system files generated by eTiceSoft or for downloading the archive file.

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	YES if provider's PPP service available
Maximum number of simultaneous connections	1
TCP/IP port number	21, can be changed by the Administrator
Deactivation by the Administrator	YES
Characteristics of the client software	Standard FTP client ETiceSoft software
User sessions and rights	1 can be changed by the Administrator + 1 system for ETiceSoft

V.2.1.3 TELNET Server

Role: This server provides for monitoring in real time information on the operations currently being processed by MIIWeb. It can be used as a diagnostic and optimisation tool.

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	YES if provider's PPP service available
Maximum number of simultaneous connections	1
TCP/IP port number	23, can be changed by the Administrator
Characteristics of the client software	Standard TELNET client
Deactivation by the administrator	YES
User sessions and rights	1 can be changed by the Administrator + 1 system for ETiceSoft

This service must be deactivated.

It must only be used in exceptional circumstances !

V.2.1.4 SMTP Client

Role: This client service enables MIIWeb to connect to a non-secure SMTP message server (no session or account identification codes), and to leave an eMail there for an addressee identified by his messaging address. The client service complies with the description of the SMTP protocol specified in RFC (2)821 and RFC (2)822.

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	YES if a PPP connection is made with a provider
Maximum number of simultaneous connections	1
TCP/IP port number	25
Maximum number of addressees per eMail	1 maximum (no copies can be sent, cannot broadcast)
Deactivation by the administrator	YES
Server characteristics	SMTP without authentication
Maximum number of characters contained in the message	100 characters
Parameters which are essential for the service to operate	Domain name of the SMTP server (if the DNS client is operational) Or SMTP server's IP address
Maximum number of characters in the addresses of eMail addressees	29 characters in total

V.2.1.5 DNS Client

Role: This client service enables MIIWeb to connect to a domain name resolution server, to convert a domain name (or URL) into an IP address, to be able to connect to it if necessary (e.g. : Domain name of the SMTP message server to leave an eMail).

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	YES if PPP connection made with a provider offering the service
Maximum number of simultaneous connections	1
TCP/IP port number	53
Deactivation by the administrator	YES
Server characteristics	DNS without authentication
Connection parameters	IP address of the primary or secondary DNS server entered manually via ETiceSoft or the MIIWeb advanced configuration pages or configured automatically by the DHCP client if it is operational and the DNS parameters are known to the DHCP Server.

V.2.1.6 DynDNS Client

This function provides for using the services of a Dynamic domain name Server. (DynDNS redirection)

This service such as that offered at the address (recommended) www.dyndns.org provides for registering MIIWeb giving a name to its IP address, from which MIIWeb can be accessed without needing to know its IP address attributed by the Provider, even when it changes.

This very useful service may be subject to a subscription independent from that of the services of the Provider to which MIIWeb is connected; Crouzet or Mecacel accept no responsibility for this service.

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	YES if PPP connection made with a provider offering the HTTP service
Maximum number of simultaneous connections	1
TCP/IP port number	80 by default, (http)
Deactivation by the administrator	YES
Server characteristics	DynDNS Server with authentication (login + password)
Connection parameters	Username, Host Nom and Passwords, defined on subscribing to the DynDNS service

V.2.2 - UDP Services

V.2.2.1 DHCP Client

Role: This client service enables MIIWeb to connect to a DHCP server, to identify itself automatically on a TCP/IP network

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	NON
Maximum number of simultaneous connections	1
Deactivation by the Administrator and the Supervisor	YES
UDP/IP port number	68
Server characteristics	Standard DHCP (RFC 2131) with DNS parameters taken into account
Connection parameters	Must be activated in MIIWeb (WEB configuration page or via EticeSoft)

V.2.2.2 System Configuration Server (UDP Config Server)

Role: This UDP server provides for updating the MIIWeb's firmware (system formatting), for changing or reading MIIWeb's IP parameters or for detecting it on the local network.

Characteristics	Operating Limits
Operational with a PPP connection (connection via modem)	NON
Maximum number of simultaneous connections	1
Deactivation by the administrator	Only on a specific order
UDP/IP port number	8001, fixed
Characteristics of the client software	EticeSoft
User sessions and rights	Rights determined by MIIWeb's firmware

V.2.3 - Security of the TCP/IP Transactions

V.2.3.1 Overview of MIIWeb's Security

The http, FTP and TELNET services are accessed through a session which must have been started using a username and a password.

Only the administrator can change the http, ftp or telnet session codes.

The file system is protected under normal circumstances; however, the standard MIIWeb version cannot guarantee total security of the embedded data if the file system is accessible.

Furthermore, CGI requests transmitted using the HTTP 1.0 protocol, although encrypted at the ISO/OSI 7 level, can be captured and possibly decrypted by a third party and this for any MIIWeb version.

The CROUZET Automatismes or MECACEL companies can in no event be held responsible for piracy or for misuse of MIIWeb whether dangerous or not by a third party. The security of the network in which it is installed is the sole responsibility of the user or installer.

V.2.3.2 Http Sessions

There are three distinct levels of connection, associated with different rights :

Session	Authorised Operations
Operator <u>Rights :</u> Minimum Factory Codes : LOGIN : user PASSWORD : user	Pages accessible and interaction authorised: <ul style="list-style-type: none"> - Remote maintenance - Monitoring (visualising states) without being able to change the state of the system - Archiving, without being able to delete the archive file
Process Supervisor <u>Rights :</u> Middle level Factory Codes: LOGIN : respo PASSWORD : respo	Pages accessible and interaction authorised: <ul style="list-style-type: none"> - IP configuration - Remote maintenance with the possibility of changing the state of the IX words (writing) - Monitoring (visualising states) with the possibility of changing the state of the process monitored - Archiving, without being able to delete the archive file
Administrator <u>Rights :</u> Maximum Factory Codes: LOGIN : admin PASSWORD : admin	Pages accessible and interaction authorised: <ul style="list-style-type: none"> - IP configuration - Advanced configuration panel (activating services, password management ...) - Remote maintenance with the possibility of changing the state of the IX words (writing) - Monitoring (visualising states) with the possibility of changing the state of the process monitored - Archiving, including the possibility of deleting the archive file

V.2.4 - Communication via RTU MODBUS

Role : MIIWeb incorporates the functions of an **RTU MODBUS** master only capable of using data of the 16-bit word type contained in the slaves (maximum 31 on any one segment), each identified by an unique address.

If the MIIWeb's MODBUS functions are used, then MIIWeb must be the sole master in the MODBUS network! (Single-master field bus)

IIWeb does not incorporate any MODBUS application layers other than the « gateway » and 16-bit word monitoring functions.

The physical liaison between MIIWeb and the RTU MODBUS slaves is of the wire type (RS485) without opto-isolation.

The line termination impedance is included in MIIWeb and is of the resistive type - value : 120 Ohms. It remains permanently connected.

Characteristic	Values
MODBUS Protocol supported	RTU MODBUS
Type of MODBUS peripheral	Master
Physical layer	RS485 without isolation
Transmission rate	300 to 57600 bauds set using ETiceSoft
Parity	Configurable (None, Even, Odd) using ETiceSoft.
Type of data useable	16-bit WORD
MODBUS Function Used	0x03 : Read Multiple Registers 0x16 : Preset Multiple Registers
Line termination impedance	120 Ohms Resistor
Maximum number of words capable of being read	100 (1 per event if all the events are used for MODBUS) + all the OX words of 8 Milleniums connected to MODBUS.

V.2.4.1 « MODBUS Gateway » Function

Role: This function enables MIIWeb to read the content of a 16-bit word in an RTU MODBUS slave and to recopy it into another slave at another address (or into an IX word in the Adjacent Millenium).

This function is managed by event. The recopy only takes place under a condition specified by the user using the EticeSoft software.

If a MODBUS read or write error occurs, an error is notified in the log the first time it occurs with a given slave. The corresponding event number is also recorded.

V.2.5 - Dialogue with the Millenium

V.2.5.1 Dialogue with an Adjacent Millenium II

MIIWeb is connected to the rear plate BUS of an extendable Millenium II (24V DC) and identifies itself as an M2WEB XC10 module, having the same exchange words and bits as an XC03 module from the Millenium II software workshop point of view.

The connection is identical to that for an XC03 Module.

V.2.5.2 Dialogue with the Millenium via RTU MODBUS

MIIWeb can manage and exchange data on all the available exchange words with a maximum of 8 Milleniums connected to an RTU MODBUS network in which it is imperative that MIIWeb be the Master.

It is imperative that all the Milleniums be fitted with the same MODBUS XC03, XC04, XN03 or XN06 extension module.

It is imperative that they are configured as RTU MODBUS slaves (connected by RS485 on 2 wires), that they have distinct RTU MODBUS addresses, and has the same RTU MODBUS communication parameters (baud rate, parity...)

In these circumstances, it is possible to display the states of the internal words from the remote maintenance page.

V.2.5.3 Automatic Time Setting

By default, after the initialisation phase, MIIWeb synchronises its system date and time to that of the first Millenium registered or other MODBUS Slave PLC(in EticeSoft) to MIIWeb and at regular intervals (every 5 minutes at the most).

However, if a communications fault should occur between MIIWeb and the Millenium or PLC used to synchronise the time, MIIWeb uses its system clock, which is reinitialised every time power is applied, as its internal time reference (dating for archiving, etc...).

V.2.6 - Data Exchange by MODEM

V.2.6.1 Types of MODEMS and Related Functions

MIIWeb can communicate by MODEM GPRS or STN, the MODEM is connected to the DB9 RS232 socket in the top right.

It is imperative that the MODEM interpret the AT commands defined by the V.25ter, GSM 07.07 and GSM 07.05. Standards, moreover, to guarantee that MIIWeb operates correctly with the MODEM, the latter must have been certified by the MECACEL Company.

It may be possible to subject a MODEM to the compatibility tests on request, and on providing a sample (however, Mecacel reserves the right to refuse certification or to invoice for it).

A list of certified MODEMs is already available.

Used with a MODEM connection, MIIWeb can exchange data using a PPP connection (Peer-to-Peer).

MIIWeb behaves like a PPP client. It tries to make a connection to an Internet access provider to make it accessible from the Internet as a Server.

The client PPP connection is programmable or can be made manually (from MIIWeb's embedded WEB site) :

- Permanent connection: As soon as MIIWeb is powered, it attempts to connect to the provider's server. If the attempt fails, it is repeated indefinitely at regular intervals until it succeeds.
- Intermittent connection: MIIWeb attempts to connect over a time frame expressed in terms of a connection start and end time; these connection and disconnection times are programmable from ETiceSoft.
- Connection deactivated : By default, when MIIWeb is powered up, this connection is inactive, however, a client PPP connection from MIIWeb's WEB site can be attempted, so the connection request is manual, from MIIWeb's embedded WEB site (MIIWeb's Supervisor or Administrator may have access to it)

PPP connection identification protocol with the Provider : CHAP, PAP, none, with or without configurable TCP heading software compression depending on the driver used (firmware).

NB : The prices and fees for GSM or GPRS communication are to be borne by the customer and are separate from the Provider costs which are also to be borne by the end customer.

V.2.6.2 SMS Management

Two conditions must be met to be able to send an SMS using a GPRS MODEM connected to MIIWeb:

- 1) The MODEM connected must be capable of sending SMSs, and in particular SMS encrypted in PDU, by interpreting the AT commands.
- 2) The SMS service must be included by the operator who opened the communication line and in the corresponding fee, in the contract to which the user of the MODEM connected to MIIWeb has subscribed.

Operating Limits :

The SMS messages generated by MIIWeb may not be longer than 100 characters.

The addressee's telephone number must be entered in international format. With the + symbol replacing the 00 at the start.

Example: +33691679867

Or must refer to a permanent SMS service whose number of coded on 5 figures.0

SMSs are edited using the EticeSoft software

V.2.7 - Alarms

V.2.7.1 Description

MIIWeb can inform the user by eMail or SMS when one of the following events occurs:

Event	Media	Comments
MIIWeb powered up	SMS	Can be deactivated via EticeSoft
Communication problem with one of the Milleniums registered with MIIWeb Soft	eMail - SMS - Fault displayed on the WEB page	Only the first occurrence of the fault is displayed on the WEB page MIIWeb tries to send the fault by eMail and by SMS
Archiving problem : No disk space remaining	eMail - SMS - Fault displayed on the WEB page	

The parameters of the addressees to be notified of malfunctions are set using eTiceSoft and the results of warning notification attempts are recorded in the page showing the last 20 events.

V.2.7.2 Limitation

The alarms are only notified by eMail or SMS on condition that these services are accessible to MIIWeb (SMTP server for eMails or GSM or GPRS MODEM connected for SMSs).

V.2.8 - Archiving

V.2.8.1 The File

This is a text file in the tab tab return format; tab : column separator; return : line separator; compatible with most spreadsheet software.

Its structure is presented below :

MIIWeb Serial Number MIIWeb Name				
Date	Time	Name: Variable 1	Name : Variable 2	Name : Variable N...
Day/Month/Year	HH :MM	0	13452	1627
Day/Month/Year	HH :MM	1	13	16
Day/Month/Year	HH :MM

As soon as the status of a variable is archived, all the others are also archived.

Its size may vary from a few bytes to several tens of Megabytes, with the limit being the amount of space available on the Compact Flash board embedded in MIIWeb.

When there is insufficient space on the compact flash board, an alarm message is displayed on MIIWeb's menu bar.

V.2.8.2 Downloading

The purpose of this operation is to copy the archive file to a PC connected to MIIWeb, via any FTP client or from the downloading too in the ETiceSoft software.

The FTP session only opens on condition that the sessions codes defined by MIIWeb's system administrator were correctly entered when the FTP client connection was made.

Depending on the connection type (GSM, DSL, Ethernet...), the time necessary to complete the download varies according to the size of the archive.xls file contained in MIIWeb.

Only one single FTP client must be connected to MIIWeb at any given moment.

VI - Maintenance

VI.1 - Maintenance operations

VI.1.1 - Free disk space management

Inside the WebServer, stands a Compact Flash card (8 bit bus compatible) for archiving data and system configurations.

On this card (called HDD), stored all files of a project definition, firmware and archives files.

The memory space available on this card is 32Mbytes.

The Archives files stored are the following:

- Archive.txt which contains the archived event's data.
- Logfile.txt which contains, if the corresponding check box of the project defined with eTiceSoft workshop checked, the events and data of the Logbook.

The size of these files increase with time. So after a certain time, it can fill all the disk memory space, leading to stop archiving.

In this case, a specific alarm occurs in the logbook, and the WebServer tries to send an SMS (if GPRS modem is connected and correctly initialized) and a Mail to the person defined in eTiceSoft workshop.

It is important to notice that this limited disk memory space is shared with WebServer's configuration files (and particularly the monitoring Web pages data) and archive files.

If there's not enough available free memory disk space, loading or modifying a project in the WebServer can lead to a FTP download error in eTiceSoft workshop download manager when user tries to download his project.

When free disk space is under 100000 byte, the WebServer set a system alarm indicating that disk is full. It then tries to send an alert eMail (and SMS if a GPRS MODEM is used) and stop archiving data (stop logfile too).

To avoid those problems, it is necessary that the WebServer administrator periodically download and delete archive and logfile from the WebServer. It can be done in two ways:

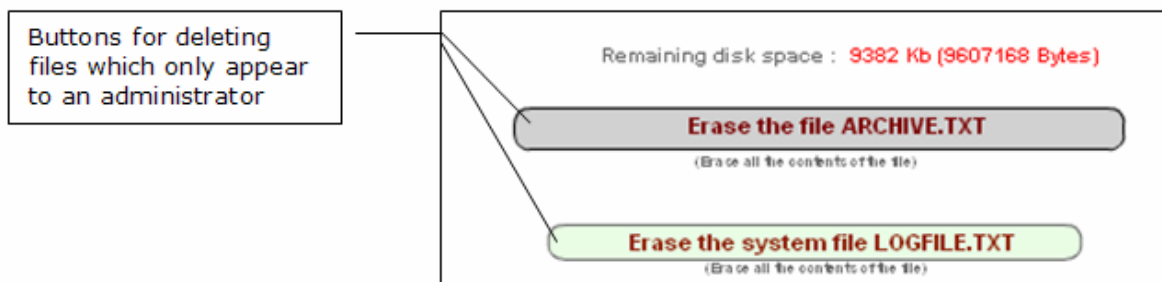
Notice :

If free disk space is too low (0 free bytes), it can lead to Web Server malfunctions (No web session can be open, cannot download any project...).

In these very rare cases, WebServer needs a complete firmware programming. This procedure can be done from eTiceSoft workshop using factory codes as explained in the "update procedure of the WebServer" application note (PDF file on the software CD – section – doc).

VI.1.1.1 Deleting archive files from on line (from the Web)

Open an administrator Web session to the WebServer using your Web browser.
In the menu bar select "Archiving", and wait about 1 minute to see the memory manager panel under the trend window.



In red colour the remaining compact flash disk space appears.
To delete a file, just press then corresponding button "Erase the file".

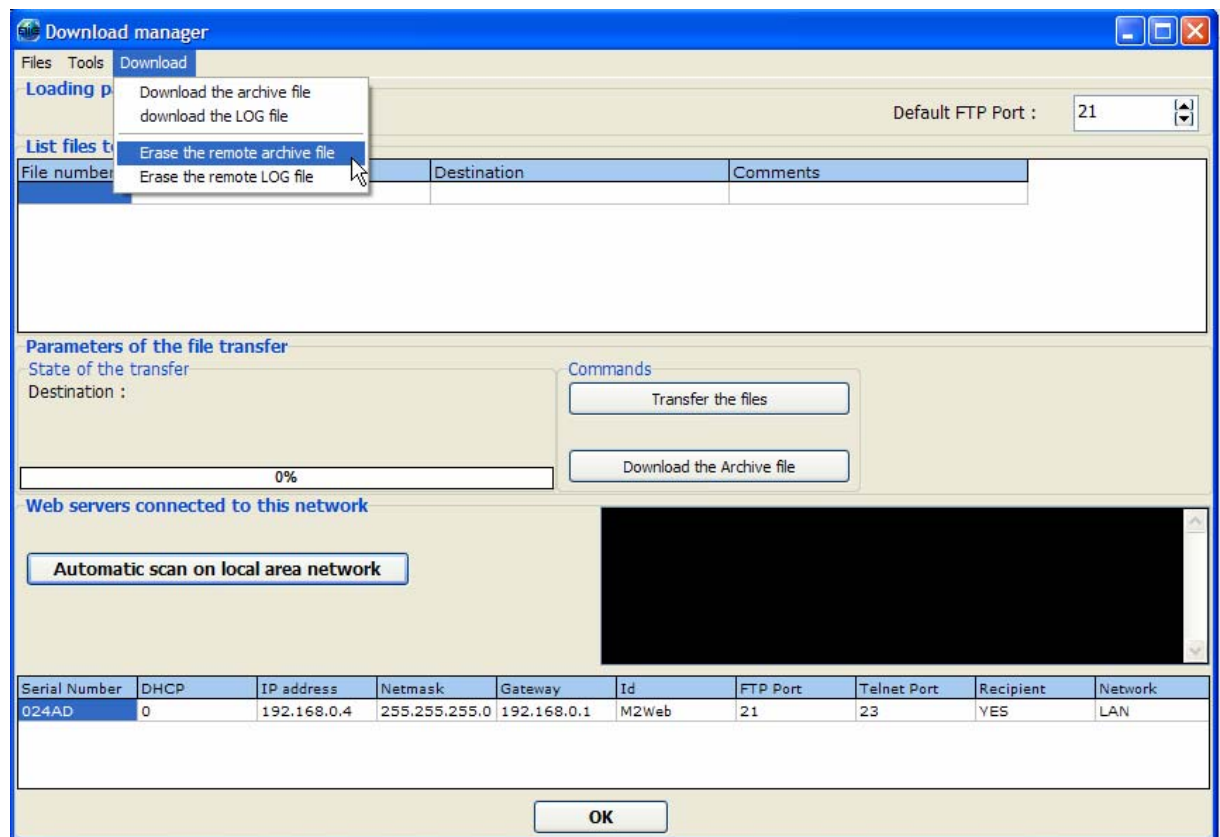
Be careful! This operation will destroy all the data of the files and reset it, so it useful to download it before using an FTP Client or eTiceSoft workshop.

Resetting a file can take several seconds and it is possible to verify that reset action is correctly done after 1 minute looking at the increase of remaining disk space.

VI.1.1.2 Deleting files using eTiceSoft workshop

Open eTiceSoft workshop and open the download manager.

Scan the Webserver on the LAN or add it manually if the WebServer is connected to a WAN (because the automatic scan does not work in this case).



Then click on download menu -> Erase the remote archive file

The software then tries to connect to FTP Server of the Web Server and then ask for session codes identification. Fill fields with administrator session codes.

The selected file is then deleted from WebServer's Compact flash disk.

VI.1.2 - Updating the Web Server

The WebServer use a powerful multitask real time operating system (RTOS kernel) with a specific firmware.

This kernel and this firmware have a version number corresponding to a eTiceSoft workshop release version number.

A new installed version of eTiceSoft leads to a firmware update of the WebServer.

The current version of eTiceSoft workshop, firmware and RTOS version is stored in the file info.ini in the directory eTice/eTiceSoft of the software install dir. A modification of one of this information leads to firmware update procedure.

The firmware update procedure can be done from eTiceSoft workshop using factory codes as explained in the "update procedure of the WebServer" application note (PDF file on the software CD – section – doc).

The update procedure can take several minutes and must be done on a local area network with correct IP addresses.

To do this update, it is needed to follow exactly the procedure described in the dedicated application note.

VI.2 - Important notices

VI.2.1 - Powering

The WebServer can be connected to an adjacent Millenium II+ XT20 24V DC via its contiguous extension port.

In this case, the same 24V DC alimentation bloc must be use for the two devices to make possible the system synchronisation procedure.

If a power fail occurs during less than 1 second, a synchronisation failure may happen between the two devices. Then the WebServer should not exchange correctly data with the adjacent Millenium II+ and a warning message appears in the logbook.

To avoid or resolve this problem, the power must be shut down for more than 10 seconds and then established normally.

VI.2.2 - Using a MODEM

The WebServer can control a STN or GPRS MODEM certified by MECACEL.

Every modification or load of a new project using a MODEM reset passwords and eventually LAN IP addresses of th WebServer.

Le WebServer peut piloter un MODEM GPRS ou RTC certifié par MECACEL.

In the case of using a 24V DC MODEM (ex : FASTRACK M1306B, GDW15...) it is recommended to use the same 24V DC alimentation bloc than the WebServer (and eventually the adjacent Millenium). This assures the correct initialisation of the WebServer at power up.

With a MODEM connected to it, the WebServer realise, at power up or after reboot, a serial of complex operations with the MODEM to guarantee its optimal use (automatic detection of communication parameters, line status, PIN Code, Measure of reception level...). This phase can lead to several reboot of the WebServer increasing system initialisation time (sometimes more than 5 minutes).

After initialisation, synchronisation tests are periodically done to check MODEM status. If a MODEM malfunction is detected, it is notified in the logbook. These tests can only be done while no MODEM connection is established.

In the case of a PPP Client connection, (WebServer is connected to an ISP), after several hours of a continuous connection, the ISP often disconnect the WebServer to avoid abuses. Then the WebServer detect this case, and tries to reconnect itself immediately.

Using the PPP Server (function reserved for redundancy use only), it is strongly recommended to wait 2 minutes between two incoming connection, because the WebServer check and synchronise the MODEM after each connection closure to prepare it for next incoming connection.

NOTICE :

Automatic closure of the PPP Server session: If no incoming data from the client are transferred through the link for more than 60 seconds, then the WebServer close the PPP Connection. Then client needs to reset the connection to the WebServer. In fact, the client just have 60 seconds to open a HTTP or FTP session since the PPP connection is established to the WebServer.

A synchronisation test is periodically done leading to PPP Server deactivated for 2 minutes.

VI.2.3 - Using MODBUS

The WeServer integrates functionalities of a MODBUS RTU RS485 master, electrically not isolated from the field bus.

Then, on long distances, electromagnetic perturbation and particularly electric and electrostatic discharges can occurs. In this configuration it is strongly recommended to insert an MODBUS opto isolated repeater to avoid system destruction or malfunction.

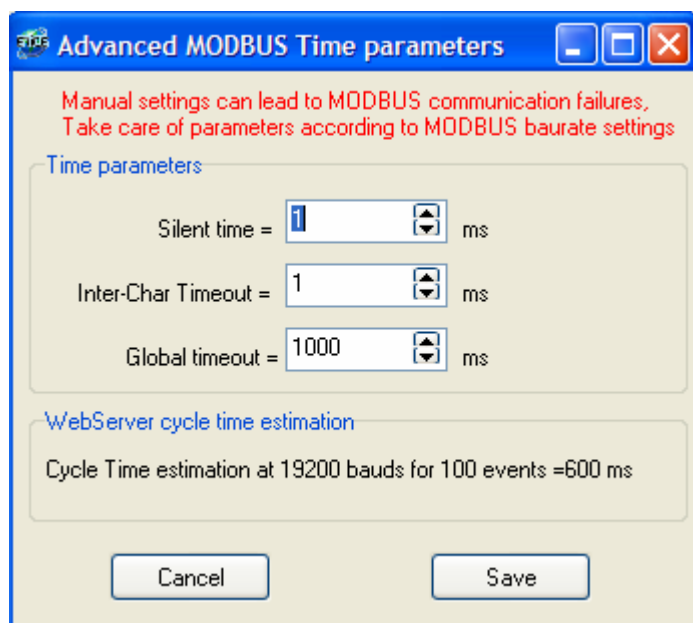
The WebServer, after its initialisation phase, read data from the MODBUS network from slave it must interrogate while normal scan cycle to realise a network diagnostic.

It's only after this sequence that events management becomes operational.

By this way, if some slaves does not answer correctly WebServer waits for TIMEOUT described in MODBUS specifications, increase delay time before normal operation and scan cycle.

The MODBUS network diagnostic is periodically done after 100 normal scan cycles.

In the configuration panel of a project (with eTiceSoft), it is possible to change manually MODBUS delays using the button "Advanced settings":



Press « save » to take this value for the creation of the « configuration file » in the project.

Comment:

Manual settings can lead to system communication malfunction if delay manually set are less than MODBUS specification values depending of the selected baudrate.

VI.2.4 - WebServer TCP/IP security notes

Data exchanges between the WebServer and a web browser, even if protected by password and encoded at ISO/OSI 7, can be analysed and decoded by a hacker.
So:

The CROUZET SAS or MECACEL companies can in no event be held responsible for piracy or for misuse of MIIWeb whether dangerous or not by a third party. The security of the network in which it is installed is the sole responsibility of the user or installer.

VI.3 - Critical use cases

This section describes WebServer's comportment when an external problem or malfunction occurs (e.g: MODEM disconnected, PPP Link failure...) to help the user to solve the problem.

VI.3.1 - MODEM RS232 link broken without any PPP connection in progress

Rising conditions of the critical use case:

- MODEM already connected and correctly initialized
- No PPP Connection in progress (PPP Server or PPP Client)

Possible event leading to this critical use case:

- Physical link to MODEM is broken (RS232)
- Power failure of the MODEM
- MODEM communication settings have been changed.

WebServer's answer in this case:

The WebServer periodically check that the MODEM is correctly connected and its configuration is corresponding to the WebServer's settings (approximately every 15 minutes).

If the MODEM does not answer right to synchronisation test, then WebServer apply the following actions:

- 1) MODEM's RS232 configuration detection attempt
- 2) If detected, synchronisation attempt
- 3) If a GPRS MODEM is used, check PIN code status and GSM network reception status.

If at least one of this action fails, then the WebServer indicates in the advanced configuration panel, in the MODEM section, this text: "MODEM PIN/PUK ERROR"

In all cases the periodical MODEM check is done each 15 minutes approximately.

VI.3.2 - MODEM or ISP link broken during a PPP Client connection

Rising conditions of the critical use case:

- MODEM already connected and correctly initialized
- A PPP Connection is in progress with an ISP (with STN MODEM or GPRS via APN)

Possible event leading to this critical use case:

- Physical link to MODEM is broken (RS232)
- Power failure of the MODEM
- MODEM communication settings have been changed.
- ISP link is down
- GSM network reception level is too low
- STN Link is broken

WebServer's answer in this case:

The PPP Client of the WebServer continuously checks the PPP connection status, if for 5 minutes, no valid information is exchanged between the WebServer and the ISP, then the WebServer hangs up the link with the ISP (sending AT commands ATH, +++...).

When the link is down,

If the PPP Client is in automatic mode (connection program activated), then the WebServer systematically tries to establish link to the ISP, if it fails it retries until the connection condition defined in the connection program ends.

If the PPP Client is in manual mode (connection forced from the configuration Web page), then the WebServer systematically tries to establish link to the ISP

The following message appears in the logbook:

PPP Link status
ISP Link broken...

When link is down, the WebServer still periodically checks the MODEM status.

VI.3.3 - MODEM or PPP Client link broken during a PPP Server connection.

Rising conditions of the critical use case:

- MODEM already connected and correctly initialized
- A PPP Server connection is already opened or connection procedure is in progress

Possible event leading to this critical use case:

- Physical link to MODEM is broken (RS232)
- Power failure of the MODEM
- MODEM communication settings have been changed.
- ISP link is down
- GSM network reception level is too low
- STN Link is broken
- The client link is broken

WebServer's answer in this case:

After MODEM status check, the WebServer tries to synchronise the MODEM, if this procedure fails, the WebServer retries 15 minutes later.

While the MODEM is not synchronised any incoming connection fails.

After a link broken, it is needed to wait about 2 minutes to make a new attempt of connection to the WebServer's PPP Server.

Remind:

Automatic closure of the PPP Server session: If no incoming data from the client are transferred through the link for more than 60 seconds, then the WebServer close the PPP Connection. Then client needs to reset the connection to the WebServer. In fact, the client just have 60 seconds to open a HTTP or FTP session since the PPP connection is established to the WebServer.

VI.3.4 - Powerfail during or after an eTiceSoft data transfer

Rising conditions of the critical use case

- WebServer is online
- A data transfer is in progress from the download manager of eTiceSoft

Possible event leading to this critical use case

- Network link is broken
- Powerfail of the WebServer
- The WebServer is rebooting during file transfer

WebServer's answer in this case:

The data transfer should fail, so the WebServer does not have enough files to work normally.

It is needed to wait about 2 minutes to restart the transfer from the eTiceSoft download manager.

It is possible that in this case, the WebServer uses its factory settings:

IP Address : 192.168

Gateway : 192.168.0.1

mask : 255.255.255.0

factory administrator session codes :

login : admin

password : admin

VI.3.5 - MODBUS Slave malfunction

Rising conditions of the critical use case

- WebServer is initialised
- MODBUS Network is used in the project

Possible event leading to this critical use case

- MODBUS Slave disconnected from the MODBUS field bus
- MODBUS Slave settings changed

WebServer's answer in this case:

WebServer is cyclically interrogates MODBUS slaves used in the project.

If a slave does not answer it is put in quarantine to be interrogate during the diagnostic sequence.

A message appears in the logbook showing the event which has a problem with this MODBUS Slave.

VI.3.6 - Static Disk is full (HDD Full)

Rising conditions of the critical use case

- Le WebServer est sous tension et la phase d'initialisation est terminée
- Le WebServer ne peut plus ouvrir de session http
- Le logiciel eTiceSoft propose une mise à jour alors que aucune nouvelle version du logiciel n'a été installée et que aucun nouveau projet n'a été transféré depuis plus de 10 minutes

Possible event leading to this critical use case

Les fichiers d'archivage occupent tout l'espace disque

- Archives files uses all disk space
- Nobody has deleted it, even if alarm messages rised in the logbook.
- The new project is too big for free remaining disk space

WebServer's answer in this case

The limited disk space is used for archives files and system files, if the disk is full, it can't work well because it cannot access the internal disk drive.

In this very critical and rare case, it is needed to follow the factory programming procedure of the WebServer (see application note of this CD).

Notice: After the factory programming procedure is done, the WebServer reset with factory settings (IP address, session codes...).

VI.3.7 - System clock is not synchronised

Rising conditions of the critical use case

- WebServer is correctly initialised
- System clock is not synchronised

Possible event leading to this critical use case

- Clock source defined in the project's configuration is disconnected from the Network.
- MODBUS Slave used for clock synchronisation doesn't have right exchange tables.
- If clock source is the adjacent Millenium II, then it should be disconnected or a power fail has occurred for less than 1 second.

WebServer's answer in this case:

System clock is synchronised at initialisation and periodically (every 5 minutes), if the device used to synchronise the clock is disconnected, then the clock cannot be synchronised.

This clock is used for dating the archives and logbook data.

By default, the WebServer's system clock is set with 00h00min00seconds the 01/01/2066.

It is possible to set the system clock from advanced configuration panel in administrator Web session only.