BITT SCADA 2008

Supervisory Control And Data Aquisition

Software package for an early radiation monitoring control center

by BITT Technology

BITT Technology
Wienerstraße 70
A-2104 Spillern
Tel.: 0043/ 2266/ 80216
Fax.: 0043/ 2266/ 80216 12
office@bitt.at
www.bitt.at

BITT-SCADA-2008

V1.0.RC3

Booklet

14.08.2008

Content

1 Purpose of this document

This document is primary a tech manual. So it does not describe how to use BITT SCADA, but it describes what is good to have in mind when using BITT SCADA! For help using BITT SCADA (after finishing the “first steps”), please use the built-in online help which can be seen as user documentation! The online help is available in English and German by default as well as the complete front-end. All other documentation and backend software is completely in English. The backend and technical documentation is assumed to be used by technicians who usually have the necessary English skills.

2 Introduction

„BITT SCADA 2008“ is a software package for an early radiation monitoring control center. The abbreviation “SCADA” (Supervisory Control And Data Acquisition) explains its features briefly. “BITT SCADA 2008” acquires data from measuring stations and provides visualization as well as the control of stations is possible.

2.1 Main features

- Data can be acquired from any measuring station developed by BITT technology. These mainly are: RSDL (DataLogger for gamma probe), autonomous solar station (RS03S), “Aerosol Measuring Station” (AMS) in version AMS02, AMS02M and AMS03, as well as the new developed “Electrostatic Universal Radiation Monitor” (EURM). For information about these products please have a look at the specific product folders.
- An Alerting Tool developed by BITT Technology can be used to send alerts via SMS or MAIL. Alerts are generated depending on user defined trigger. With the BITT Technology alerting hardware also trigger IOs can be used. e.g. to control a hooter.
- The acquired data is stored in a SQL database and visualized through a web server.
- For specific purpose the “BITT SCADA 2008” can also provide the collected data through a FTP server and an optional direct database access for custom queries.
- Every Browser can act as a client. The web page is optimized for MS Internet Explorer 6 but also tested with MSIE 7, Firefox 1.5.x / 2.x, Netscape 7.1 and Opera 8.51.
- Modular structure, so the system is easily upgradeable and adaptable.
- Optional data export in EURDEP format 1.3 and 2.0.

2.2 System architecture

The following figure shows the system architecture of BITT SCADA in its full scale! Every module is covered by an extra license. So every customer gets the ordered modules, thus not all together by default!

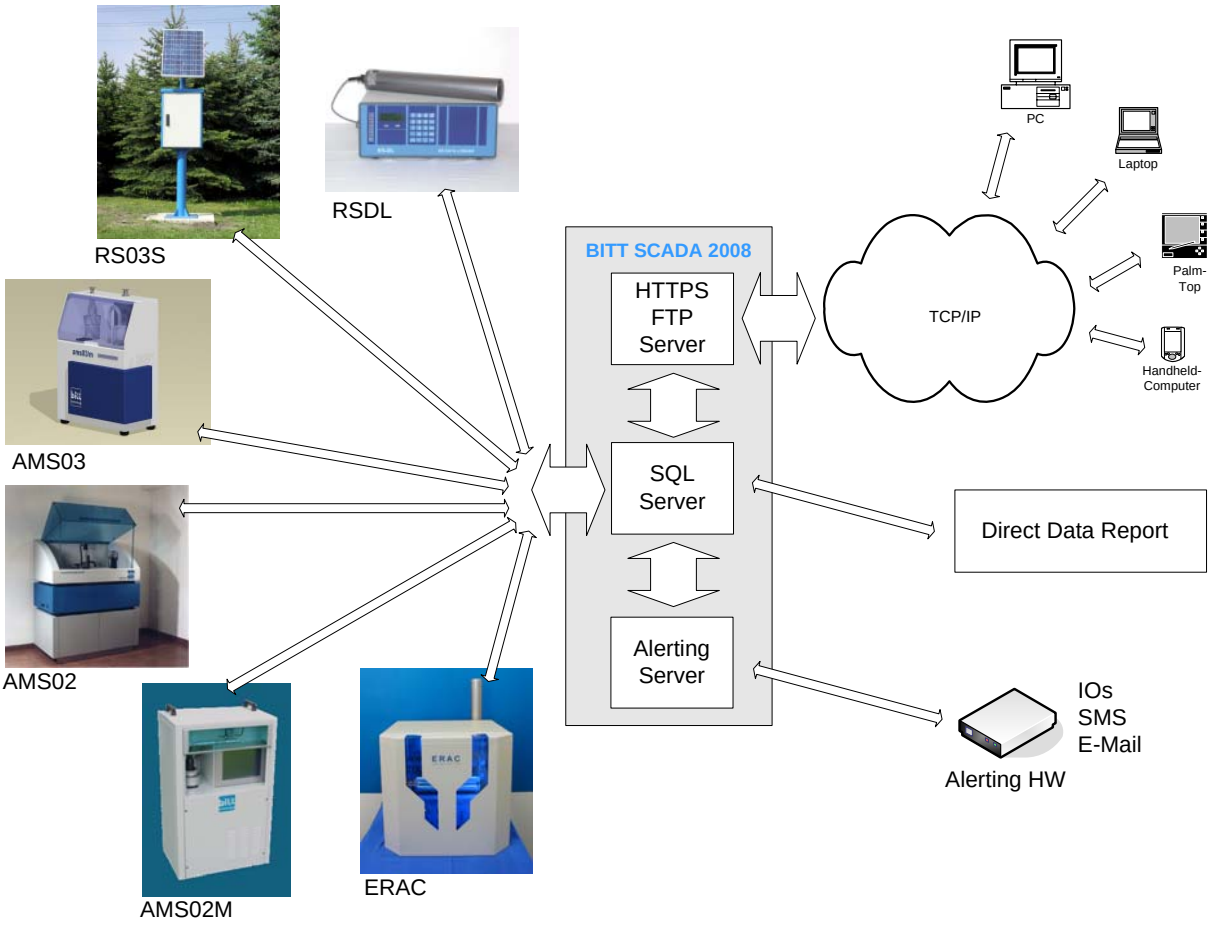


Fig. 1 System architecture „BITT SCADA 2008“

3 First steps and prerequisites

Normally a ready to use BITT SCADA 2008 server is delivered to the customer. If the clients aren't configured by BITT Technology too the customer and/or the user respectively should read this chapter first to get an appropriate visualization.

a) Accessing the web based visualization is possible over domain names and/or one or more IP addresses. The determination of the access methods is done in consent with the customer.

b) The data is always secured via SSL. This means the connection to the web server and the database. So connect to https://domain_or_IP_of_bitt_scada_server/. If not otherwise agreed the SSL certificates are created by BITT Technology. The CA (certificate authority) isn't distributed with the root certificate update of MS Windows and therefore not a registered CA! This leads to a failure message of the browser first! We recommend accepting the certificate temporarily! Don't store the certificate or take any other actions. The CA as well as the web server certificate is valid for ten years from delivery on. BITT SCADA is still functional, even with an expired certificate, but the browser will give a warning message about it!

c) Then you have to get through the first phase login (web server authentication). The username and password are handed over to the customer separately. The first phase login is the same for all users that should have access to the server. The first login has the purpose to hide the purpose of the web page to unwanted guests. This is especially necessary if the web server is exposed to a public network (eg. the Internet). Storing this username/password combination at the client within the browser isn't rated as a high security risk at all. After a successful first phase login you'll see the second phase login screen (BITT SCADA authentication).

d) Now we recommend installing the public certificate of the BITT CA. To do this, just go to the following page: https://domain_or_IP_of_bitt_scada_server/data/programme/. Here you find the specific certificate and two important client programmes. To install the certificate of the BITT CA click on "cacert.crt" and follow the instructions of the browser and/or the OS (operating system). Most browsers have their own certificate storage, so that you'll probably have to redo the installation if you want to use another or further browser. After installing the CA's certificate close the browser! To test the proper installation of the certificate restart the browser and go to the BITT SCADA server. No failure message should come up now! But still there is one exception: If one uses another IP or DNS than given within the web server's certificate, then the browser will report that the two names don't match. This can be the case if the certificate is generated for the use from the Internet via IP or DNS "X" but the access is done through the Intranet via IP or DNS "Y".

e) The next step is to complete the second phase login which is personified. Thus it's recommended to assign every person its own username and password. If not otherwise agreed, one supervisor account is handed over to the customer. With this account the customer is able to create as many as user accounts as required. It's not recommended to store the second phase login username and password at the client (eg. in the browser or OS)!

f) After the successful second phase login the user is ready to use BITT SCADA. When using a screen resolution of 1024x786 it's recommended to switch the browser into the full screen mode. Most browsers support this by pressing "F11". Using a screen resolution of less than

1024x786 isn't recommended! Each user can adopt the resolution settings to ones own good within the configuration menu. In general the use of BITT SCADA can be done intuitively.

g) The JRE (JAVA Runtime Engine – Version 6.0 or higher) is required for viewing charts. You can obtain the latest version from www.java.com or directly from the BITT SCADA server (https://domain_or_IP_of_bitt_scada_server/data/programme/) where only the Windows version of the JRE is available. The web visualization is always tested with the JRE version at the BITT SCADA server!

h) For viewing spectrum files it's necessary to install a special viewer at the client. The newest version of "AMS02view" can always be found directly at the BITT SCADA server under the following link: https://domain_or_IP_of_bitt_scada_server/data/programme/. If you want to update to a new version you have to uninstall the old version of AMS02view first. (Up to now AMS02view is only available for MS Windows!)

4 Main components

4.1 Server Hardware

For less than 5 concurrent connections to BITT SCADA a Windows XP certified home PC has usually enough performance. The customer can widely choose the components of the server, up to a high performance server. The main condition is that the server has to be suitable for Microsoft Windows.
The minimum hardware requirements are:

- CPU: 1.5 GHz
- RAM: 1 GB
- Hard disk: 120 GB + 10 GB for each AMS02 Station.
- Network interface: 100 Mbit

Recommended additional hardware:

- Backup media: DVD-writer, streamer, etc.

4.2 Operating System (OS)

Microsoft Windows is used as OS. Which version, depends on the customer! BITT SCADA has already been installed on Windows XP Professional, Windows XP x64 Professional, and Windows 2003 Server. The OS is installed with one supervisor account. The password can be changed from the customer after delivery in one's sole discretion. All updates from Microsoft, available at delivery, are installed!

4.3 Web server

Usually Microsoft's IIS or Apache are used. They are installed side by side, thus a switch between them can be done by BITT Technology if desired. Which web server is currently used is shown at the bottom line of the web application. The version of the web server varies from one OS to the next because the OS included IIS is used, if not otherwise expressly agreed! In case of Apache version 2.0.49 is used!
In any case the web server is configured for SSL a will not accept unencrypted connections. Each customer gets its own SSL certificate from BITT Technology. The customer is free to use another certificate of choice! Such a change is not included in the standard license, if not otherwise expressly agreed!
For controlling (e.g. start, stop, etc.) the web server please use the IIS control panel or the Apache service monitor!

4.4 Database

If not otherwise expressly agreed, MySQL 5.x is used as database. The database is used for storing all kind of data. This means configuration settings, vocabulary, measuring data as well as log data and certain passwords. If your license includes direct data access you might have a look at the enclosed database model, where all databases and tables are explained. The here fore necessary account is provided separately.
External connections to the database are also secured by the means of SSL. Connections that don't leave the server (e.g. from the web server to the database) are not secured.

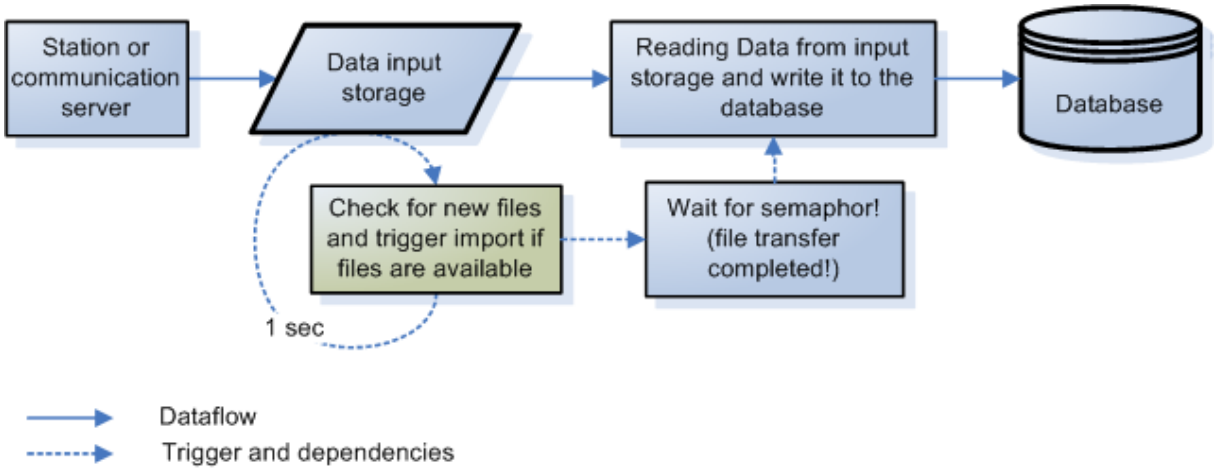
4.5 FTP Server (optional)

If agreed, a FTP server is configured to provide the collected measuring data in form of text files. This is optional and has to be ordered separately.

4.6 Parser and control software in general

Data from all kinds of stations are transferred to the main central in many different ways. Usually files are used to send data! These files have to be imported into the database what is done by the means of many different parsers. According to your license the necessary parsers have been installed on the BITT SCADA server. If not otherwise agreed the scope of delivery covers all BITT device types which have been ordered by the customer. The main different device types are shown in chapter “2.2 System Architecture”.

All parsers are working after the same principle. Data is transmitted from a station directly to the BITT SCADA server or via a separate communications PC and put into a storage which is usually a directory structure. A program called “timecontrol” is polling the input directory and triggers the import after the file transfer has been completed. Then the parser writes data into the database. A more detailed description as well as flowcharts can be found in the next chapters!



4.7 Alerting Tool Software

This software module is an optional feature of the BITT SCADA system. Users are able to generate alarm triggers via the web based visualization of BITT SCADA. These triggers can target all kinds of measuring quantities and other data which is stored in the database of the BITT SCADA system. Users can also configure to receive alerts via mail or SMS for each specific alarm trigger. The Alerting Tool which is running on the BITT SCADA server, generates the alerts depending on the user configurations. To be able to send alerts by mail, a mail server (SMTP) must be available. For SMS alerting the BITT Technology alerting hardware module is used which is also capable of triggering IOs controlling e.g. a hooter.

4.8 Alerting Hardware

The alerting hardware consists of a GSM modem to be able to send SMS alerts and a Trigger IO board. All the hardware is installed in a 19'' enclosure and can be installed in every 19'' cabinet. The alerting hardware is connected via a USB cable and a modem cable to the BITT SCADA server. Also an external power supply is needed.

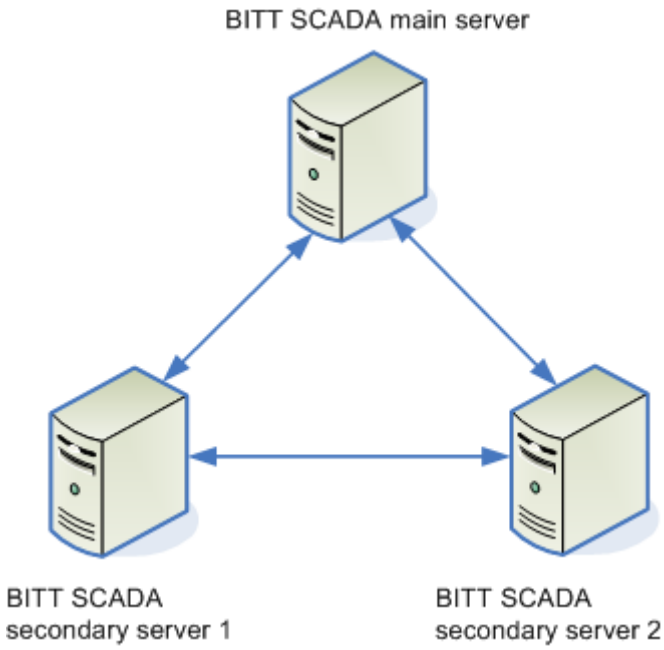
key features: 8 inputs (3.3V – 20V) [currently no software support]
8 outputs (250VAC, 5A)

4.9 EURDEP export

The optional EURDEP export software module provides functionality for manually or automatically exporting data conforming to the EURDEP standards 1.3 and/or 2.0 for a system independent exchange of radiological or meteorological data, collected with the BITT SCADA hard- and software.

5 Inter-centre communication and administration

It is possible to maintain more than one BITT SCADA server within the customer's early radiation warning system! In this case, it's necessary to connect the servers via a permanent TCP connection. This connection is used from the servers to negotiate the hierarchy within the network as well as to exchange measuring data. On the next figure you can see an example configuration with three BITT SCADA servers. More than one main server must not exist. The assignment in the example is arbitrary.



5.1 CentreControl

Switching between functions can be done via the web application (front-end) and directly from the server machine via the program called "CentreControl" (back-end). Be aware that supervisor rights are always necessary to switch between main and secondary function! The back-end program version offers also the possibility to override security functions. The security functions normally don't allow the user to set up a second main centre. So normally the main server must be switched back to secondary before another centre can be switched to main. The configuration files can be found in the BITT SCADA top level program directory. If changing the configuration is necessary please stick to the comments in each configuration file.

6 Alerting Tool in detail

The Alerting Tool has been developed in LabWindows/CVI from National Instruments. After installing the Tool on the Bitt SCADA system the graphical user interface is located at the bottom of the screen. The program files can be found under C:\BITT-SCADA\. In the GUI of the Alarm Tool the current status of the mail Server, GSM Modem and the Trigger IOs are displayed. The Alerting Tool can be configured via an ini file which is located in the program directory like mentioned before. (timer periods, trigger IOs, and so on)

The Alerting Tool consists of 6 main threads and 2 message queues:

Message queues:

Following message queues are used for inner task communications:

Mail message queue: "Check alerts" thread sends the mail data to the "send mail" thread.
SMS message queue: "Check alerts" thread sends the SMS data to the "send SMS" thread.

Threads:

Check modem status:

This thread is periodically started by a timer. The main task of this thread is to check the status of the modem, e.g. is the modem connected, is the modem registered to the GSM network and so on. If no GSM modem is available it can be disabled in the configuration ini-file. If the modem is disabled this thread and the "send SMS" thread will also be disabled.

Send SMS:

This thread is started automatically and waits for messages in the SMS message queue. If the "Check Alerts" thread sends a message to the SMS message queue the "send SMS" thread receives it and sends the SMS via the GSM modem. After that the thread waits again for a new message. If a special exit message received, this thread will be terminated.

Check server status:

This thread is periodically started by a timer. The main task of this thread is to check the status of the mail server. This is done by creating a telnet connection to the mail server and the SMTP port. The SMTP port can be configured via the ini-file in the case of using not the standard port. If no mail server is available it can be disabled in the configuration ini-file. If the server is disabled this thread and the "send mail" thread will also be disabled.

Send mail:

This thread is started automatically and waits for messages in the mail message queue. If the "Check Alerts" thread sends a message to the mail message queue the

"send mail" thread receives it and sends the mail via the mail server. After that the thread waits again for a new message. If a special exit message received, this thread will be terminated.

Check Alerts:

This thread is also controlled by a timer. The thread checks the SMS and mail limits if one of the limits reached an error mail and SMS will be sent to administrator which are configured via the web based visualization of the Bitt Scada system. If at least one limit isn't reached the thread starts to get Trigger data and checks if alerts are available. If no alerts are available the tread terminates automatically. Otherwise the thread reads user and trigger data from database, generates mail and SMS messages and sends them to the corresponding message queue provided that the modem and/or the mail server is enabled and available.

Check trigger IOs:

This thread is controlled by a timer. The thread reads trigger IO data from database to know which trigger is turned off or on and how long. Trigger IOs can also be configured via the ini-file. The IO name and the time how long the output will be active in the case of an alarm can be set. So the IO thread knows which trigger should be turned on and of and can set the states in database and on the alerting hardware.

7 Logging

The dataparsers are usually split up in two main parts. The first part has controlling functions and
Each device type has its own set of dataparsers! So they have also their own directory for logfiles which can be found in the device-type main directory and is usually named “logs”. These logs are very detailed and therefore only stored for one month in a system like a ring buffer! For each day one logfile exists. One example for the content of such a logfile:

```
24.01.2007 01:10:32: ams02data.exe: Programmstart Automatic Mode with FileType: ME!
24.01.2007 01:10:32: ams02data.exe: Nothing to update
```

Each line is divided into 4 sections: date, time, the name of the executable that wrote the line and last but not least the message itself. Most of the messages make only sense if they are pulled together with the lines before and/or after them! The above example shows such a case: no data has been written / updated in the database for the filetype “ME” (meteorological data) of the configured AMS02 devices.

The centre control software has its own logging directory in the BITT SCADA programs top level directory! The structure is pretty much like above. The last known status of a centre also appears in this logfile besides the database! One example for the content of such a logfile:

```
17.01.2007 08:24:24: CentreControl.exe: Application closed by user!
17.01.2007 08:45:10: CentreControl.exe: Start of application!!!
17.01.2007 08:45:19: CentreControl.exe: bitt-scada-2006 (3): Main Central
```

The alerting tool software has its own logging directory in the BITT SCADA programs top level directory! The structure is pretty much like above. One example for the content of such a logfile:

```
17.10.2007 00:00:18: AlarmCenter.exe: Check GPRS - Modem Status...
17.10.2007 00:00:18: AlarmCenter.exe: Update Program Status...
17.10.2007 00:00:18: AlarmCenter.exe: Mail Server OK!
17.10.2007 00:00:19: AlarmCenter.exe: Modem Status OK!
```

These log files are only useful for maintenance as well as locating failures and faults! But of course these log files are not made for regular work. No separate explanation of the messages is available because they are detailed enough themselves! These log file messages aren’t stored in the database and therefore they are always in English!

Document history

provided by: Matthias Rötzer	date: 21.09.2009
for contents: Matthias Rötzer	date: 21.09.2009
Released by: Günter Kemminger	date: 21.09.2009