BRUKER ADVANCED X-RAY SOLUTIONS

Software Maintenance

for BCP and BIS, APEX2, PROTEUM2, and PILOT Software Packages and the Frame Buffer Computer

Purpose

These instructions cover software maintenance for Bruker AXS frame buffer computers, including configuration, customizing, security, updating, troubleshooting, and routine operating system maintenance and repair.

Responsibilities

All procedures are to be performed only by trained Bruker AXS personnel or by locally authorized persons.

Disclaimer

All configurations and specifications are subject to change without notice.

1 Instrument and Software Access by User Accounts

NOTE: This section applies to BCP, BIS, VIDEO, and other frame buffer programs.

Various computer user accounts offer different levels of access to settings and data (used with the Bruker instrument and software) according to the level of responsibility you are granted. Your organization may require certain individuals to have a full-access level, some individuals to have a limited-access level, and others to have no access. Or you may simply wish to prevent novice users from accidentally changing the alignment or calibration of your Bruker instrument. You can accomplish both by using the operating system's user management features to restrict an individual or group of individuals' user access level to the Bruker instrument.

To apply a level to a user account, create a list of all users, their computer user accounts, and the level of instrument access you want them to have (as follows).

NOTE: By default, all computer user accounts are Instrument Users. Therefore, at a minimum, certain accounts may need to be changed for full access or no access.

- **Non-User**: Any individual that is not allowed to operate the Bruker instrument in any way. By default, no computer user account is a Non-User.
- **Instrument User**: Any individual that is allowed to operate the Bruker instrument for data collection on samples but not allowed to align or calibrate the instrument (to prevent novice users from accidentally changing the alignment or calibration of the Bruker instrument.). By default, all computer user accounts are Instrument Users.
- **Instrument Administrator**: Any individual that is allowed to operate the Bruker instrument for alignment and calibration (typically also an Instrument User). By default, only the computer user account “Administrator” is an Instrument Administrator.
- **Instrument Security Administrator**: Any individual that is allowed to modify the security features of the Bruker instrument (typically not an Instrument Administrator or Instrument User). Security features are typically not activated and no one has to be an Instrument Security Administrator. By default, no computer user account is the Instrument Security Administrator.

If your organization will be using domains for computer accounts, you will have an individual that is designated as the Domain Administrator. Take a copy of your list of users and access levels and a copy of this document to your Domain Administrator. That individual will configure the accounts.

Most laboratories are not centrally administered by domains. Instead, the lab manager runs everything. Using the list of users, accounts and access levels created earlier, the lab manager can configure the accounts by following the instructions in the various sections of this procedure.

1.1 Configuring User Accounts for Non-Users

Non-Users (unauthorized individuals) are a class of user prevented from running any Bruker instrument software.

Ideally, all unauthorized individuals would be physically prevented from touching the instrument (only authorized individuals would have access to the lab). But in a large lab, or for greater security measures, you may need to prevent certain individuals (who have physical access) from using the instrument. In this case, you can make those individuals Non-Users.

By default, the Bruker frame buffer assigns all computer user accounts as Instrument Users. If you want an individual to be a Non-User, choose one of the following methods to reconfigure the software for Non-Users.

Method 1: Simple Setup

1. Install all Bruker software for personal (not common) installation.
2. For each additional user of Bruker software, copy the BrukerAXS program group to the Program folder of the new user account. Then create a “Shortcut to BrukerAXS Programs” on the new user's desktop.
3. Copy “BrukerAXS Programs” from an existing GADDS/SAXS user account to the new user’s Start menu.
   - 3.1 Go to Start > Programs > Windows Explorer.
   - 3.2 Navigate to %USERPROFILE% (typically, C:\Documents and Settings).
   - 3.3 Find “BrukerAXS Programs” under [user] > Start Menu > Programs.
   - 3.4 Right-click on “BrukerAXS Programs” and select “Copy”.
   - 3.5 Navigate back to %USERPROFILE% (typically, C:\Documents and Settings).
   - 3.6 Find [newuser] > Start Menu > Programs.
   - 3.7 Right-click on white space of right panel and select “Paste” (not “Paste Shortcut”).
4. Create a “Shortcut to BrukerAXS Programs” on the new user’s desktop.
   - 4.1 Right-click on the “BrukerAXS Programs” shortcut that you just created and select “Copy” .
   - 4.2 Find <newuser>\Desktop.
   - 4.3 Right-click on white space of right panel and select “Paste Shortcut” (not “Paste”).

NOTE: This method does not prevent Non-Users from starting a Bruker program by double-clicking in Windows Explorer. Non-Users just will not see any Bruker programs in their Start menus.

Method 2: Robust Setup

1. Create a “BrukerUser” group for your computer user accounts.
2. Assign this group to all computer user accounts that are allowed access to the Bruker software.
3. Restrict access to the BrukerAXS folder containing all of the Bruker software. The BrukerUser group needs read access. BrukerAdmin and BrukerSecurity needs full access.

1.2 Adding User Accounts for Instrument Users

Instrument Users can operate the Bruker instrument to collect data on samples. However, they cannot use configuration and alignment features. They can use APEX2, PROTEUM2, or PILOT to collect data, but BCP will only display the current configuration (therefore, the user cannot make any changes). This restriction prevents novice users from accidentally changing critical configuration settings (e.g., wavelengths and beam center) and from re-calibrating the detector.

By default, all computer user accounts are Instrument Users. To add an Instrument User account, you only need to set it up through the operating system’s user management feature and do nothing else.

1.3 Adding User Accounts for Instrument Administrator

Instrument Administrators can perform configuration, alignment, and full operation of the Bruker Instrument. These computer user accounts are members of the “BrukerAdmin” group.

By default, only the “BrukerAdministrator” account in Windows XP or the “Administrator” account in Windows 2000 is an Instrument Administrator.

To add an Instrument Administrator account, add a computer user account through the operating system’s user management feature. Then reconfigure the account for Instrument Administrator by adding “BrukerAdmin” rights to this computer account.

1.4 Adding User Accounts for Security Administrators

Security Administrators can configure the security features of the Bruker Instrument to enforce your laboratory policies. Presumably, these policies will enable your laboratory to be fully compliant with CFR 21 part 11 (FDA) and GLP. Typically Security Administrators lack both Instrument Administration and Instrument Usage rights. By default, there is no Security Administrator.

To add a Security Administrator account, add a computer user account through the operating system’s user management feature. Then reconfigure the account for Security Administrator by adding “Bruker Security” rights to this computer account.

1.5 Adding User Accounts

Computer User accounts form the basis of security for the operating system. Each user will be assigned a different user account. Each user account has access to certain programs and privileges. For example, the Administrator account has full access to everything on the computer and by default is also the Instrument Administrator for Bruker software. In contrast, the Bruker account may be configured with limited rights (that is, no access to install drivers, etc.).

By default, Bruker frame buffers are configured for local accounts. These accounts are only accessible by logging into the frame buffer. Local accounts are maintained on the frame buffer. In contrast, domain accounts are accessible throughout the network domain. Your company’s Domain Administrator maintains domain accounts remotely. When you log into the frame buffer, you are asked for the username, password, and either the computer or domain name.

Adding Domain Accounts

Because you do not have access or the privilege to do this, you must contact and provide your Domain Administrator with the following information:

- Full user name, as this name gets logged in the audit trail.
- The user's access level: BrukerUser, BrukerAdmin, and/or BrukerSecurity.
- A copy of Section 1 of this manual.

Adding Local Accounts (WinXP/Win2000)

1. Log into the Computer Administrator user account.
2. Click Start > Settings > Control Panel.
3. For WinXP, click User Accounts. For Win2000, click Users and Passwords.
4. Select the “Advanced” tab. Note that this is not the logical path (you would assume the [Add] button instead).
5. Click the [Advanced] button.
6. Highlight Users on the left pane.
7. Click Action > New User (from the menu bar).
8. Fill out the “New User” dialog box as defined by your company policies. For audit trail features, you will want to fill out the “Full name” field correctly.
9. If this user needs appropriate group rights—Bruker User, BrukerAdmin, and/or BrukerSecurity—you must add that later.
10. Click the [Create] button. The account will be created, the dialog box will be cleared, and you can enter more accounts if you wish.
11. Click the [Close] button when you are finished adding user accounts.

1.6 Adding Rights to User Accounts

Adding Bruker rights (WinXP/Win2000)

1. Log into the Computer Administrator user account.
2. Click Start > Settings > Control Panel.
3. For WinXP, click User Accounts. For Win2000, click Users and Passwords.
4. Select the “Advanced” tab. Note this is not the logical path (you would assume the [Add] button instead).
5. Click the [Advanced] button.
6. Highlight Users on the left pane.
7. Highlight and double-click the user account on the right pane.
8. Select the “Member of” tab.
9. Click the [Add] button.
10. Highlight the group to add, such as BrukerAdmin.
11. Click the [Add] button.
12. Repeat the last two steps for each additional group to add.
13. When done, click the [OK] button.

2 Sample Database and Software Access by User Accounts

NOTE: This section applies to APEX2, PROTEUM2, and PILOT software packages.

Client software programs are designed to perform only data collection on samples. Clients may run on any computer (including the frame buffer) and connect to BIS via the network.

The first task each client performs is to log in to a central Bruker sample database. Thus the User Manager of this database controls which individuals are allowed to operate the Bruker instrument for data collection on their samples (see M86-Exx092 User Manager Manual). Additionally, the computer user account must also have access to this database (see M86-Exx084 PILOT Installation Notes).

3 Software Updates

Updates are program fixes and minor enhancements. In contrast, upgrades are major enhancements and include new manuals. Updates are freely distributed to all existing, legal Bruker customers via our web site. For upgrade possibilities, contact your Bruker Sales Representative.

3.1 Web Site Updates

Any Windows XP/2000/NT software that says “Bruker” in the copyright can be updated by downloading the appropriate patch file from our web site. The patch installation is simple. Just run the .exe file. The patch will find the previous installation of our software and update the software. Should the patch be unable to find a previous version, the patch installation will fail. Therefore, these software patches are useless unless you already have Bruker software.

NOTE: You can uninstall the patch using the “unwise.exe” routine.

Some software patches may be distributed in multiple patches. For example, for updating GADDS 4.x to the latest version, you must first update to GADDS 4.0.10 and then update to the latest version using

- PhoenixUpdate3xx.exe,
- GADDSUpdate4.1xx.exe and
- GADDSMAP1.1xx.exe.

Before downloading any software patch, you must access the web site and register. A few days after doing so, you will be e-mailed a username and password to access the download page. At that point, follow these instructions:

1. Download all web patch files for your software package.

2. Execute each file to start the SETUP program. You will see the following dialog boxes. Respond as shown in the right column.

Welcome screen	[Next]
Read Me File (may be missing)	[Next]
Choose Destination Location screen	[Next]
Start Installation screen	[Next]
Installing…	This progress screen disappears when completed
Installation complete screen	[Finish]

Following are Error Messages you may encounter:

Message
"Error: The file <path\filename> could not be opened"
Reason and Resolve

- This patch is only for existing Bruker installations. You must run this patch on a machine with Bruker software already installed.
- You may have entered the destination directory incorrectly.

Message
"Error: The file C:\saxi\gaddsnew\gadds.exe is not a valid previous version and could not be upgraded."
Reason and Resolve

- The executable program may be infected with a computer virus. As all viruses attach code to program files, the update patch will not recognize any infected file as a valid previous version (the checksum will fail).
- You may have forgotten to install a required update patch first.
- You may be running a beta release of the program.
- If the problem appears to be something other than that mentioned above, contact Bruker Service.

4 Software Errors

4.1 Error Messages

During operation of the Bruker instrument, various error messages will be sent to different places, depending on the origin of the error.

If a program crashes, a Dr. Watson error displays and a copy of the error message gets sent to the event log. You should report these messages (see event viewer) along with the steps needed to recreate the error.

All device driver error messages are sent to the event log, such as errors from Bruker detector drivers (SAXAD.SYS, AT300.SYS, SCSI). While these errors are not displayed by the client application (BCP, PROTEUM, or PILOT), they typically will create another error that is displayed to the user.

Various Controller (PHOENIX, GGCS, low temp, high temp, etc.) errors display inside BIS and are also sent to the Client application (BCP, PROTEUM, or PILOT) for display to the user.

Some common (D8 system) error messages are:

Message
"Can't reset goniometer controller. Check serial link"
Reason and Resolve
Can occur when software was installed with GGCS drivers on a D8 system.

Message
"Phoenix controller is not responding or serial link problem"
Reason and Resolve
Another program (D8TOOLS) already is using COM1.

Message
"Phoenix controller is not properly configured for software"
Reason and Resolve
Something inside the file DEVICE.INI is incorrect. You must correct it before BIS will operate the instrument. See file \D8\readme.txt on Bruker Software CD.

Message
"Phoenix firmware is too old"
Reason and Resolve
BIS now requires Phoenix 3.0, 3.04 or later.

Message
"Goniometer must first be initialized with Home command"
Reason and Resolve
The angle was lost. Use either the Home or the Update command to set the angle.

Message
"Timeout waiting for reply from goniometer controller"
Reason and Resolve
Communication to the controller was lost. You may have to reboot the controller.

Message
"Please contact Bruker service to upgrade your generator firmware"
Reason and Resolve
This message is only a warning. Old generator firmware sometimes locked up the system.

4.2 Reporting Errors

BCP and BIS have a quick bug report command that makes it easy to submit software performance reports to Bruker.

Just click on the "Send to" button or File > Send command and a default bug report form is generated with many fields already filled in and your configuration file and BIS.log file automatically attached. All you need to do is fill in the problem section and click the [**Send**] button.

A MAPI or SMTP host is required for sending bug reports.

In APEX2, PROTEUM2, or PILOT, you may generate an email and send it to:

software@bruker-axs.com

5 Software Glossary

5.1 D8: Device.ini, PHOENIX.exe, & D8_CTRL.exe

Definitions

The controller firmware is the software that controls the goniometer, generator, and other components of the instrument.

Device.ini is the configuration file for all D8 firmware.

PHOENIX.exe is the controller firmware for the D8-01 enclosure.

D8_ctrl.exe is the controller firmware for the D8-02A and D8-02B enclosures.

Versions

Bruker instruments have shipped with various releases of the firmware: 2.02/19-Jun-99, 3.02/21-Nov-99, 3.03/19-Jan-00, 3.04/14-Mar-00 (for RA systems), and 3.04/11-May-00. The current release of BIS only supports release 3.08/23-Feb-2001, 3.08/16-Feb-2001, and later release. We recommend releases:

PHOENIX 3.12/15-Jan-2002

D8_CTRL 2.05/02-Mar-2005

D8_CTRL 3.02/10-Feb-2005

Check Version

To check the current version and date of the firmware:

1. Run D8TOOLS.
2. Go to Manual Control.
3. Type "RV" and press [Enter] (do not type the quotation marks).
4. Read the response in the Instrument Response section "RV3.12/15-Jan-02."

Creating Firmware Floppy

Use the Bruker Software CD to create a firmware floppy. The directory \D8Firmware contains the Phoenix Firmware. Use one of the following batch procedures:

“Make Floppy for D8-01.bat”

“Make Floppy for D8-02A.bat”

“Make Floppy for D8-02B.bat”

to create a bootable floppy diskette. This procedure creates a bootable floppy with phoenix.exe or D8_CTRL.exe, but without the configuration file: device.ini. Under the E:\ D8Firmware \PROTEUM or PILOT directory are other files. Many example configuration files, *.ini, are present. Copy the closest example to the floppy and rename it to device.ini.

The PILOT versions are:

GADDS-CS.ini	CS configuration with smaller XYZ stage.
GADDS-CS_y150.ini	CS configuration with larger XYZ stage (y is 150 mm).
HuberCradle.ini	Large quarter-circle stage.
Phi.ini	Fixed Chi stage with microscope.
Phi_Zoom.ini	Fixed Chi stage with optical zoom.
Xyz_Zoom.ini	XYZ stage with optical zoom.

The APEX2 and PROTEUM2 versions are:

Device.ini	Fixed Chi stage.
RotatingAnodeDevice.ini	Fixed Chi stage on RAG.
\X8\Device.ini	MACH3 goniometer.

Updating

Updated software is distributed via our web site and by the latest Bruker Software CD, which are discussed later. Print and read the release notes. When updating the firmware, you most likely also need to update the device.ini configuration file and maybe the application programs, such as BIS, as described in the release notes. Update the D8 firmware floppy by copying over the latest files: phoenix.exe or d8_ctrl.exe and *.v30.

Editing Configuration

After creating or updating the firmware floppy, you must edit the configuration. Use an ASCII file editor such as notepad and open the file a: device.ini. See D8 firmware release notes, the readme.txt file distributed with the firmware or firmware update.

Backup Firmware Diskette

A backup copy of the current firmware and configuration is always kept under the Bruker software tree (typically this is C:\Program Files\BrukerAXS\D8Firmware or C:\SAXI\D8Firmware). Rename the subdirectory D8 Firmware or PHOENIX to D8 Firmware.old or PHOENIX.OLD and then create a new directory called D8 Firmware or PHOENIX. Copy the contents of the firmware floppy to this new directory.

Restore a Firmware Diskette

To restore a firmware diskette, create a firmware floppy and then copy the files from the firmware backup directory to the floppy diskette. This instruction assumes the backup copy was recent—otherwise, you must create a firmware diskette and edit the configuration.

5.2 GGCS: gc.exe and defaults.su

NOTE: PROTEUM requires the GC version 3.56 or later. For a CCD detector, the GGCS Scalar card is required. If either is missing, the frame scan times will be imprecise which will, in turn, adversely affect data quality.

Definitions

GC.exe is the controller firmware—the software that controls the goniometer, generator, and other components of the instrument. Defaults.su.ini is the configuration file for the firmware.

Versions

Bruker instruments have shipped with various releases of the firmware: 3.21 to 3.56. The current release of BIS only supports release 3.56 and higher. We recommend 3.56 or higher.

Check Version

To check the current version and date of the firmware:

1. Run TALK to GC.
2. Enter “?” (Do not type the quotation marks).
3. Read the first line of the response.

Creating Firmware Floppy

Use the Bruker Software CD to create a firmware floppy. The directory \GGCS contains the GGCS Firmware. Use batch procedure “MK_GGCS.BAT” to create a bootable floppy diskette. For safety reasons, this procedure will not run by double-clicking; instead, it displays a syntax message. Use Start > Run > open: “E:\GGCS\mk_ggcs A” > [OK]. This procedure creates a bootable floppy with gc.exe, but without the configuration file: defaults.su.

Updating

Updated software is distributed via our web site and by the latest Bruker Software CD, which are discussed later. Print and read the release notes. Update the GGCS floppy by copying over the latest files: gc.exe.

Backup Firmware Diskette

A backup copy of the current firmware and configuration is always kept under the Bruker software tree (typically this is C:\Program Files\BrukerAXS\GGCS or C:\SAXI\GGCS). Rename the subdirectory GGCS to GGCS.OLD and then create a new directory called GGCS. Copy the contents of the firmware floppy to this new directory.

Restore a Firmware Diskette

To restore a firmware diskette, create a firmware floppy, and then copy the files from the firmware backup directory to the floppy diskette.

5.3 SYS drivers

Definition

SYS files are hardware drivers to control PCB boards or other computer hardware.

SCSI

Drivers needed to operate the Fairchild CCD detectors are standard SCSI drivers from Adaptec.

AT300.SYS

Driver for controlling the Roper CCD detectors. During software configuration, BCP properly configures Win2000/NT to start this driver.

SAXAD.SYS

Driver for controlling the Siemens Analytical X-ray Area Detector interface card (SAXAD). During software configuration, BCP properly configures Win2000/NT to start this driver. For very unusual situations, some registry keys can be customized. For example, you can change the detector orientation on systems where the detector is mounted sideways or upside-down (see M86-Exx008 GADDS Software Reference Manual: 13.11 SAXAD.SYS Bruker HISTAR NT Driver).

DIONTDRV.SYS

Special driver for SAXS software only. Controls the Digital-IO card for shutter and detector control. Requires DIOLIB.DLL as the GCLIB.DLL controller.

5.4 DLLs

Definition

DLLs are dynamic link libraries. They create a software layer between the application program, BIS, and the goniometer controller (or detector).

Controller DLLs

BIS uses different DLLs for different goniometer controllers. During software installation, SETUP copies the appropriate DLL to gclib.dll.

PHOENIX.DLL	For Phoenix controllers.
GGCS.DLL	For GGCS controllers.
GCDUMMY.DLL	For Dummy controller (emulator for demos).
DIOLIB.DLL	For SAXS only, Digital-IO controller.

Detector DLLs

BIS uses different DLLs for different detectors. During software installation, SETUP copies the appropriate DLL to detector.dll. Currently, the CCD detectors do not have a DLL.

HISTAR.DLL	For HI-STAR detector.
PXC.DLL	For VÅNTEC 2D detectors.
DETDUMMY.DLL	For Dummy detector (emulator for demos).

High-Temperature DLLs

BIS uses different DLLs for different high-temperature controllers. During software installation, SETUP copies the appropriate DLL to tempctrl.dll.

TCDUMMY.DLL	None. (emulator).
TCAPKHR.DLL	ANTON-PAAR KHR (NANOSTAR).
TC800EPC.DLL	Eurotherm 800 Series.
TC900EPC.DLL	Eurotherm 900 Series.
TCWATLOW.DLL	Watlow 988 Series.
TCDHS900.DLL	DCS-350, DHS-900, or MRI
TCHTK16.DLL	Socabim HTK-16

5.5 BIS

Definition

The Bruker Instrument Service is a Windows 2000 service that controls the entire Bruker instrument. Services are programs that are always running, even if nobody has logged onto the frame buffer.

Versions

Latest version is 1.2.1.12 or 2.0.0.3. We recommend running the latest version. Enhancements and bug fixes for each version are listed in the release notes (on-line).

5.6 APEX2, PROTEUM2, PILOT

Definition

Application programs (e.g., APEX2, PROTEUM2, and PILOT) are executed by the user for instrument control and data processing.

Versions

We recommend running the latest version. Enhancements and bug fixes for each version are listed in the release notes (on-line).

5.7 BCP

Definition

Bruker Configuration Program for use on all Bruker frame buffers running BIS.

Versions

Latest version is 2.0.0.3/16-Feb-2005.

Documentation

See your APEX2, PROTEUM2, or PILOT Service/Administrators Manual.

5.8 D8TOOLS & D8DOCTOR

Definition

Diagnostic and testing utility for the D8 controller. There are different versions of D8TOOLS for each D8 firmware version.

D8DOCTOR is a 21 CFR part 11 compliant diagnostic tool and is available only for 02A and 02B firmwares.

Versions

Latest versions are:

D8TOOLS 3.02/03-Feb-2005

D8TOOLS-02A 3.04/11-Mar-2005

D8TOOLS-02B 4.03/10-Feb-2005

D8DOCTOR 1.03/17-Dec-2004

D8DOCTOR 2.00/17-Dec-2004

Documentation

See M88-Exx001 D8/ADVANCE & DISCOVER X-ray Diffractometer, User Vol. 1.

See the online .pdf for D8DOCTOR.

6 Useful Operating System Information (Win2000)

6.1 Service Packs

Since the original releases of Windows XP (WinXP) and Windows 2000 (Win2000), Microsoft has made enhancements and bug fixes. About every six months Microsoft collects all these changes together and releases a service pack. Service packs are cumulative (that is, service pack 2 contains all changes in service pack 1 plus new changes). Therefore, you only need the latest service pack.

Most Bruker software requires WinXP or Win2000. The particular service pack is not important.

As of April 2005, we have tested WinXP service pack 1 only. Currently, we recommend service pack 1 and all security patches.

As of April 2005, we have tested Win2000 service packs 0, 1, 2, 3, and 4 and all work fine. Currently, we recommend installing service pack 4 and all security patches.

For Microsoft Internet Explorer, we recommend installing the latest version, latest service packs, and all security patches.

Some service pack rules:

- You cannot install a lower service pack when a higher service pack is already installed.
- Anytime you insert the Win2000 CD to install files, files from the current service pack will be installed. This is a major improvement from Windows NT, where you had to reapply the current service pack after inserting the NT CD.
- Installing a service pack will force a PC reboot.
- Do not use the uninstall service pack option after you have added system software (see the second rule above).

6.2 Event Viewer

Definition

Windows XP/2000 records information about various occurrences within the system into Event Viewer's three log files: System, Application, and Security. The System log file records events related to system operations, most often associated with device drivers and services. The Application log file records events related to applications, programs, and utilities, not native Windows XP/2000 tools. The Security log file records events related to security and auditing (we can ignore the security log).

Usage

Always check the log file whenever some driver or service failed to start or an application crashed. Some common examples are:

- HI-STAR driver failed. You will see various SAXAD messages in the System log.
- VIDEO software fails. You may see various METEOR or CORONA messages in the System log.
- DHCP fails. You will see various DHCP messages in the System log.
- PROTEUM or PILOT crashed. You will see a Dr. Watson message in the Application log.
- Double-click on the single line of the message to get the full details.

6.3 Windows XP/2000 System Information

Definition

Windows XP/2000 System Information is a read-only window into the hardware configuration of your Windows XP/2000 system. The various trees will display information on system summary, hardware resources, and IRQs:

System Summary

OS name, Version, Processor (type and speed), BIOS Version, Memory, etc.

Hardware Resources

Conflicts/Sharing: All modern PCs can handle IRQ chaining (that is, sharing of IRQ) among different boards.

IRQs

Used system resources for IRQ assignments. Great place to find resource conflicts.

6.4 Registry

The Registry is a database that stores hardware, software, and user system configuration information. The Registry replaces the Windows 3.11 INI files (system.ini, win.ini, config.sys, *.ini) with a single database file to simplify management and configuration tasks. Unfortunately, if any software corrupts the Registry, everything is lost, and the computer usually fails to boot. Before editing the Registry, you should know what you are doing or you may suffer dire consequences.

Bruker Karlsruhe makes extensive use of the Registry. All program settings are stored in the Registry—(e.g., User preferences, Sample settings, Instrument settings, etc.).

Bruker Madison makes more limited use of the Registry with our software products:

- User preferences may be stored in the Registry. If these settings are lost, you need not worry, as they do not affect data, data quality, data processing, or results, and they can be reestablished easily.
- Crystal or sample settings are stored in the Bruker sample database (PostGreSQL 8.0).
- Instrument settings are stored in BCP's BrukerInstrument.ini file (only one exists).

- Driver settings must be stored in the Registry. SAXAD driver and others use the Registry.

You can use one of the Registry Editors to view, find, or modify the Registry keys and values. Start > Run > “RegEdt32” or “RegEdit” > [OK]. RegEdt32 displays in tree structure and provides commands to edit Registry security. RegEdit displays in Explorer structure and has better searching capabilities. Reasons to run the Registry Editors are:

- To customize the detector driver, such as SAXAD or AT300.
- To clean up and remove any Siemens keys.
- To fix VIDEO installation (board or camera type).
- To fix an operating system, driver, or performance setting.
- To change the RegisterOwner value.
- To remove uninstall options from the Control Panel's Add/Remove applet.

6.5 Emergency Repair Disk (ERD)

In Win2000, you use the Backup application to access the utility for creating an ERD. By default, this utility updates the DOS initialization files and the setup log, but the utility can also back up Registry hives. When you select the Registry-backup checkbox, the utility automatically saves the hives to the \%systemroot%\ repair\regback folder but not to your ERD. If your Registry becomes corrupted or erased, you can use the files in this folder to restore just your Registry and avoid a lengthier restoration of the Win2000 System State data, which typically occupies a minimum of 200 MB of storage. To restore System State data, you need to use the Win2000 Recovery Console. (For more information, see Zubair Ahmad’s, “The Windows 2000 Recovery Console,” http://www.win2000mag.com/, InstantDoc ID 7250. For more information about System State, see Zubair Ahmad’s, “Backing Up and Restoring the System State,” http://www.win2000mag.com/, InstantDoc ID 7664).

6.6 Emergency Repair Process (Win2000)

The Win2000 Emergency Repair process is similar in that you run Win2000 Setup from the CD-ROM or startup disks and choose the Repair option. You then can choose Fast Repair or Manual Repair. Fast Repair tries to repair system files (using the checksum method and setup.log), the boot sector on your system disk, and your startup environment. Fast Repair also checks the Registry files. If a Registry hive has a problem, Fast Repair automatically copies the hives backed up in the \%systemroot%\repair folder.

Manual Repair, an interactive subset of Fast Repair, does not check the Registry hives. It does let you perform one or all of the other three Fast Repair options above: verifying system files, inspecting the boot sector, and checking the startup environment.

6.7 Emergency Repair Process (NT)

Reference: (taken from Windows NT Power Toolkit, page 98-100, 153)

At this point you are unable to boot your system after making a change to the Registry (either from manually editing the Registry or from installing or configuring software and/or drivers). Instead of the logon screen, you see the dreaded BSOD (Blue Screen Of Death) or STOP message. Understanding this hieroglyphic-like screen is not necessary. Some key indicators will greatly aid the investigation. The second line of the STOP message lists the type of error encountered. The error will read “Unhandled User exception” or “Unhandled Kernel exception” followed by some address information. This information focuses the troubleshooting search. Unhandled User exceptions involve user-mode operating system software, whereas Unhandled Kernel exceptions relate to the operating system, third-party software drivers, or hardware.

The third and fourth lines of the STOP message indicate what caused the failure and the associated address or addresses. Look for a filename in these lines.

NTOSKRNL.SYS	NT Operating System Kernel.
ADPU160M.SYS	Adaptec SCSI driver for Ultra160 SCSI.
AIC78U2.SYS	Adaptec SCSI driver for Ultra-2 SCSI.
AIC78XX.SYS	Adaptec SCSI driver for older SCSI.
SAXAD.SYS	Bruker HISTAR driver.
AT300.SYS	Bruker AT300 driver.

The best escape option that Microsoft provides is the Last Known Good Configuration. When, you boot Windows NT, you are presented with an option to press the spacebar to utilize the Last Known Good Configuration. After you press the spacebar, you are presented with a menu from which you may choose saved configurations. The Last Known Good Configuration means that, based on the last configuration, your system was able to get to the initial logon screen (your PC booted successfully). It does not mean that your Registry was evaluated against some criteria for goodness—rather, that your boot appeared to be successful as far as Windows NT was concerned. With Last Known Good Configuration, you should be able to log into the system to repair potential damage done. You must press L to use the Last Known Good Configuration.

The second restoration method is The Emergency Repair Process, with or without the Emergency Repair Disk (ERD). To restore Windows NT using the ERD, follow these steps:

1. Find your NT Distribution CD, three setup floppy disks, latest ERD disk for your PC, Adaptec SCSI driver disk, and NT Service Pack (Bruker Software CD).
2. Boot Windows NT using the three setup floppy disks or the CD-ROM, or by running the WINNT.EXE program. We recommend using the floppies.
3. The Windows NT Setup screen appears, asking if you would like to install Windows NT or repair a Windows NT installation. Press the R key to choose the repair option.
4. You will be asked what tasks you would like the setup program to complete. The tasks include inspection of the Registry files and the startup environment, verification of the Windows NT system files, and inspection of the boot sector. Choose the tasks you want performed (using the arrow keys to navigate and the Enter key to toggle selection). When you are ready to continue, Press the Enter key when the Continue (Perform Selected Tasks) option is highlighted.

NOTE: We strongly suggest that you first try inspecting the Registry files, the startup environment and the boot sector. Do not restore any Registry hives on the first try. If this fails to restore the NT computer, then repeat this procedure and try the other options. Restoring a Registry hive means that you must re-apply all Registry changes since the ERD disk was created (except for whatever caused the system to crash). Verification of system files will restore the original NT system files (service pack 1) and you will need to reapply the latest service pack.

5. Press the Enter key to allow the Windows NT Setup program to find the floppy and hard disk controllers. Then press the S key to specify additional controllers. Then select “Other driver on OEM floppy (exact wording unknown).” Load the Adaptec SCSI driver from the Adaptec floppy. Select the “U2” driver for Ultra-2 controllers. Select the other driver for older controllers.
6. The Setup program asks if you have the ERD available. If you have the ERD, press the Enter key. You will then be prompted to insert the ERD into the floppy drive. If you do not have the ERD, press the Esc key and the Setup program will attempt to detect the Windows NT installations that are on the hard drives. It then prompts you to select which Windows NT installation to repair.
7. Follow the instructions presented to you, inserting the ERD (if one is available) when requested.
8. When the emergency repair process is complete, remove the ERD and press Ctrl+Alt+Delete to reboot the system.

6.8 Performance

For NT performance issues, refer to Windows NT Power Toolkit Chapter 20: Tuning and Optimizing Windows NT, pages 391 to 418. For automatic performance tuning, we recommend the AutoPilot program.

6.9 Lost Password Problem

This problem ranges from annoying to critical. If you just installed the operating system and realized you forgot the administrator password you assigned during Setup, a quick reinstall will take care of the problem. You will lose an hour or so at worst. If you have been using the system for a while, however, you could have a real problem, particularly if the system contains additional user accounts.

The easiest way to solve a lost password problem is to log into another account that has Administrator group privilege and use User Manager to change the password for the account with the lost password. If you cannot log into any account with Administrator privilege and the computer is on the network, try logging onto a different computer using an account with Administrator privilege and then use User Manager to change the lost password.

If you can stand to lose all the accounts on the computer (usually not a problem on a workstation), one of the easiest fixes is to delete the SAM hive, which stores the accounts. When you restart Windows 2000, you will have a new Administrator account with a blank password.

If you installed the Recovery Console (RC) and configured it for automatic administrative log-on, you should be able to boot the RC, delete the file %systemroot%System32ConfigSam and restart. Otherwise, boot the system with a floppy to gain access to the folder and delete the file. If the system drive is formatted as FAT, you can use a bootable DOS diskette. If it is formatted as a New Technology File System (NTFS), you will need an NTFS driver to enable you to access the disk. Check out NTFSDOS and ERD Commander at the web site of Austin, Texas-based Winternals Software LP. Both of them will let you boot the system and gain access to NTFS volumes.

If you cannot afford to lose the existing accounts, you will need to take a different approach. Visit the Winternals Software web site for ERD Commander Professional and NTRecover with NT Locksmith for additional options that will let you reset the password and regain access to the system.

Other options are:

- Use the ER Procedure to restore a SAM database with a known password (NT 4.0).
- Use the GetAdmin hack (for NT 4.0 SP3 or earlier). Some SPs fixed this problem.
- Use the LINUX hack. Runs off a floppy, scans the SAM, and allows you to change the password. The file you are looking for is LoPhtCrack.
- Use third-party software, such as www.lostpassword.com, www.elcomsoft.com or http://l0pht.com.

BRUKER AXS INC. • 5465 EAST CHERYL PARKWAY • MADISON, WI 53711-5373 • USA
TEL: (+1) (800) 234-XRAY • TEL: (+1) (608) 276-3000 • FAX: (+1) (608) 276-3006
E-mail: info@bruker-axs.com • www.bruker-axs.com

BRUKER AXS GMBH • ÖSTLICHE RHEINBRÜCKENSTR. 49 • D-76187 KARLSRUHE • GERMANY
TEL: (+49) (721) 595-2888 • FAX: (+49) (721) 595-4587
E-mail: info@bruker-axs.de • www.bruker-axs.de

BRUKER NONIUS BV • OOSTSINGEL 209, 2612 HL DELFT • THE NETHERLANDS
TEL: (+31) 15 215 2400 • FAX: (+31) 15 215 2500
E-mail: info@bruker-nonius.com • www.bruker-axs.com

NOTE: All configurations and specifications are subject to change without notice.