

Security Entry Solution Version 3.0

APPENDIX

SES - System Reset Procedures

Restarting a Single Remote Workstation:

If you have only *ONE* computer in your gatehouse and are connected to the SES system through a telephone line, press the [ESC] key at the SES Main Menu and exit the program. Once you are at a black screen (called the DOS prompt), shut off *BOTH* your computer and modem. The power switch for the computer is located on its front face. The power switch for the modem (usually *white* device that lets your computer “talk” to another through a phone line, it is about six inches wide, one inch tall and has eight red *and* green lights on it) is located on the back right of the device. Once you have shut off *BOTH* units, turn them back on. Your computer will automatically restart and connect to the main gate house through the modem.

Restarting a Single Local Workstation:

If you have *MANY* computers in your gatehouse but have only one monitor (computer TV display screen), chances are that you also have a monitor / keyboard switch box. This box allows you to switch your monitor / keyboard between the different computers on the network. This *black* box has six green lights on the front and measures about one foot wide, four inches tall, and has one push-button and one switch on the front of it. Press the push-button a few times to switch the monitor to the computer you want to restart, and press the [ESC] key on the keyboard to exit the SES program. Once you are at a black screen (called the DOS prompt), shut off the computer. If there is a modem attached to this computer, shut it off as well. Once you have shut off *BOTH* units, turn them back on. After the computer successfully restarts, change back the monitor switch box to its original setting.

Restarting the ENTIRE Network:

1. Have all remote gates exit the SES program and then shut off their computers and modems.
2. Use the monitor switch box in the main gate house to exit out of the any other active SES programs.
3. Turn off all computers and modems in the main gate house *except* for the SES server.
4. Exit the SES server by pressing the [Ctrl]+[Alt]+[Del] keys simultaneously and then select [S] for shutdown.
5. Turn off the SES server. Make sure all the other computers and modems are OFF!!!
6. Turn on the SES server and wait a couple minutes until it is fully started.
7. Turn on each computer / modem workstation in the main gate house, one at a time. Wait until each is fully started.
8. Once all the workstations in the main gate house are fully started, you can instruct the remote gates to restart.



Modem



Monitor Switch Box

Backing Up

Periodic backup of the SES system is highly recommended. You should schedule a complete backup every week. The same tape may be reused each week. Every three months you should do a complete backup and store the tape *off-site* in a safe and secure place.

1. Have all remote gates exit the SES program by pressing [ESC] and then shut off their computers and modems.
2. Use the monitor switch box to exit completely out of *ALL* other active SES programs except for the *Backup Station*.
3. Insert a backup tape into the drive of the *Backup Station* in the guard house.
4. Exit the SES system on the *Backup Station* by pressing [ESC].
5. At the menu select the “**BACKUP**” option. This will enter the backup software and start the backup.
6. Make absolutely sure that no other stations will use the SES system during the backup process!!!
7. Once the backup is complete, all other workstations can be started.

SES Error Codes and Descriptions

A Note on Error Codes

Occasionally there may be events that happen to your computer that may cause an error code in the SES. Some of these errors will require some sort of technical support to help recover from the error.

Recovering from Backup

Any of the errors listed below that require the file to be rebuilt can also be easily fixed by restoring it from a recent backup. A mass storage backup device is installed on all SES Systems by **The Feick Corporation**. A regular daily or weekly backup can save money, time and aggravation. If you experience a fatal error, just restore from your most recent backup that was *not* having the error.

Error Code	Description	Action
2	I/O Error: Disk read/write error. The file was not found or the file that was to be opened is damaged.	If you are on a network, make sure the network connection is still active, otherwise the Btrieve file needs to be rebuilt.
3	File not open: The file trying to be accessed is not open.	Check the number of files in the CONFIG.SYS, increase and see if the error stops.
4-11	<i>Internal index related errors.</i>	If errors persist, files need to be rebuilt.
12	File not found: The file specified was not found.	Check to make sure you are in the correct directory and the data files are all there.
13	Extended file error: (Not applicable)	
14	Pre-Image open error: The system could not open the pre-image file used to protect file transactions.	Make sure the disk is not full. A pre-image file (.PRE) may have been deleted, the Btrieve file must be rebuilt. There is not sufficient access rights in this directory.
15	Pre-Image I/O error: The system could not write to the pre-image file.	Check for disk space. The pre-image file may be damaged and have to be rebuilt.

16	Expansion error: (Not applicable)	
17	Close error: The system is unable to properly close the file, possible due to another person updating it while open or there is a damaged drive.	Check for disk errors.
18	Disk Full: There is no room left on disk to add records.	Free up disk space.
19	Unrecoverable Error: The data file is damaged and it's integrity cannot be guaranteed.	The file must be rebuilt.
20	Record manager inactive: The Btrieve record manager was not started.	Use the STARTSES or SESMENU batch file to start the SES, <u>not</u> the EXE name.
21-23	Buffer length errors: Internal file error.	Seek technical support.
24	Page size error: Btrieve may have been started with an invalid parameter.	Use the proper batch files to start the SES.
25	Create I/O error: The file cannot be created because the disk may be full or the user does not have the proper access rights.	Free up disk space or grant the proper access rights.
26-29	<i>Index or Record length errors.</i>	Seek technical support.
30	Not a Btrieve file: The file specified was not created by the system. The file is either severely damaged or has been copied over by mistake.	Restore the proper file or seek technical assistance.
31-35	Extension/Directory errors: (Not applicable)	
36-40	Transaction file errors: (Not applicable)	
41	Operation not allowed: Transaction in progress on file.	Try operation later.
42	Incomplete accelerated access: The system was terminated while files were opened and the data file was not closed properly.	The file must be rebuilt.
43-51	Internal file errors: The system experienced a file error.	Seek technical assistance.
52	Error writing cache: An I/O error occurred with the disk.	Check disk for possible errors and/or seek technical assistance.

54	Variable page error: The system could not read all or part of the variable length portion of the record. The file is most likely damaged.	The file must be rebuilt and/or seek technical assistance.
55-56	Internal file errors: The system experienced a file error.	Seek technical assistance.
57	Expanded memory error: The system received an error from the computers Expanded Memory Manager.	Test expanded memory, check for other applications using expanded memory.
58-59	Internal file errors: The system experienced a file error.	Seek technical assistance.
60-79	<i>Not used.</i>	
80	Conflict: The update of the record cannot be performed because another user has updated the record since the system read it.	Exit the current operation and try again.
81	Lock error: The system was unable to lock or unlock the record requested.	Exit the system and try again.
82	Lost position: The record pointer is no longer valid.	Exit the system and try again.
83	Read outside transaction: (Not applicable)	
84	Record in use: The record the system attempted to lock is already locked by another user.	Exit the system and try again.
85	File in use: The system attempted to open a file, lock a record or access a record that is in use by another user.	Exit the operation and try again.
86	File table full: The record system's file table is full.	Seek technical assistance.
87	Handle table full: The operating system cannot assign a handle for the file being opened.	Increase the FILES statement in the CONFIG.SYS.
88	Incompatible open mode: (Not applicable)	
89-92	<i>Not used.</i>	
93	Incompatible lock type: (Not applicable)	
94	Permission error: The system cannot perform a function due to an operating system restriction.	Check file attributes and user access rights.

SES Technical Bulletin: Video Capture Problems

Problem: Video Capture randomly stops working within the SES.

Solution: The Capture Card is not damaged, or bad. Every time you press [F4] to capture within the SES Resident File Area the SES resets the Capture Card. Occasionally the Capture Card refuses to listen to this reset. A temporary fix has been implemented. A program that comes with the Capture Card called SVIA resets the card every time.

Directions for Implementing FIX:

1. Exit the SES Software.
2. Once at a MS-DOS Prompt, type **'cd \svia' + [ENTER]** or **'cd \util\svia' + [ENTER]**
3. At the C:\SVIA> or C:\UTIL\SVIA> prompt type **'SVU' + [ENTER]**
4. Once you see the SVIA Menu use the Arrows to choose Preview & press **[ENTER]**
5. If an error appears make sure your camera is on and the cable is hooked up.
Otherwise you should see a picture appear. Press **[ESCAPE]**.
6. The choose Quit.
7. Answer **'Y'** to save settings.
8. Type **'cd \' + [ENTER]**
9. Type **'SES' + [ENTER]**
10. Retry the capture Operation.

SES Disaster Recovery Plan

Table Of Contents

Introduction 9

Equipment Protection and Safeguards 9

 AC Power 9

 Power Surge/Lighting Strike 10

 Environment: Moisture, Dust and Temperature 10

 Replacing Equipment 10

Software Protection and Recovery 11

 Backing Up the System 11

 Restoring Data from Back Up 12

Total System Failure/Switch to Manual Operation 12

 Procedures for Site Operation with NO **SES** system 12

24 Hour / 7Day Service Coverage 12

Summary 13

Introduction

The **Security Entry Solution (SES)** has two very important components that are required for its secure and reliable use. One is the *equipment*, which is the computers, printers, keyboards and monitors that were installed with the system. These items give the **SES** an environment to run in and allows it to display information, take and store call authorizations and print passes.

The second component is the *data*, this is the information that is stored in the computer that tracks the names and addresses of the residents, as well as all of the call authorizations recorded by the system. Without the *data* that has been entered and called in, the system would be nothing more than a collection of computer equipment.

Because your **SES** system is comprised of these two vital pieces, the following recommendations are structured to protect *both* the equipment and data in the simplest and most effective way.

Equipment Protection and Safeguards

The **Security Entry Solution (SES)** is comprised of many pieces of computer hardware all of which are selected to help the system run in the most reliable and efficient manner.

Unfortunately, time, and the environment, take their toll on computer equipment and some type of failure will eventually occur.

Most computers are generally designed for business, home or laboratory use, they do not age well being run 24 hours a day, seven days a week in a less than ideal environment like a guard house. Due to the high use and exposure, we have found that the average life expectancy of the gate house computers is three to four years. We have found that the recommendations that follow help the computers achieve a long life span.

AC Power

All of our equipment is installed using an UPS (Uninterruptible Power Supplies) to supply power to the system. The primary function of a UPS is to provide working power to the computer system during short “black-outs” and “brown-outs”. As soon as a drop in voltage is detected by the UPS, it uses its internal battery to supplement or replace the power and keeps the computers running without any interruption.

A UPS also functions as a power filter by dampening periodic spikes and transient voltage “noise”. Both spikes and “noise” degrade semi-conductor material over time and will shorten the life of the computer.

The UPS packs have a limited effective life span for both the battery and the spike/“noise” filtering circuitry. The UPS device should be tested regularly by simulating a power outage, if the device does not work properly, it should be replaced. The UPS should be replaced regardless of its performance within one year of reaching the maximum life span indicated by the manufacturer (the general current life span of a UPS is three to six years).

To protect against a long-term power failure (longer than fifteen minutes), it is recommended that a power generator be properly wired into the gate house. There are a wide variety of generators available and a qualified electrician would be the best person to recommend and install one that would meet the power needs of the entire gate house.

Power Surge/Lighting Strike

The UPS is designed to filter small surges and line “noise”, however, a strong surge or lighting strike can easily fuse the internals of the UPS and travel on the sensitive computer equipment. All UPS packs should be plugged into a “lightning arrester” type power strip. These “lightning arrester” power strips are designed to dissipate power surges and disconnect power from attached equipment if the surge is too great (as in the case of a lightning strike). Any SES Equipment not connected to a UPS should be plugged into a “lightning arrester”.

All “lightning arrester” surge suppressors have indicators on them so that they can easily be checked for proper operation. If the “lightning arrester” does not indicate normal operation, it should be replaced. The “lightning arrester” used should be one with a lifetime warranty and some type of “attached equipment” policy that will insure your computer equipment in case the unit fails and the computer equipment is damaged as a result.

Any telephone lines connected to the computer equipment should also be protected by a suitable surge suppressor designed for use with a telephone line. Many of the “lightning arrester” power strips come with telephone surge connectors also.

Environment: Moisture, Dust and Temperature

A very serious life limiting factor for computer equipment is the environment they exist in. Most computers manufactured today are not designed for any type of harsh environment and are generally expected to be installed in a business office, a home or a school. Dust, salt air, moisture and high temperatures all contribute to the premature failure of computer components.

All of the main computer cases should be kept in an enclosed cabinet with high air flow (duct fans) and dust filters. The cabinet’s internal temperature should not exceed 80° F and the relative humidity should be 50% to 70%.

Replacing Equipment

In the event a component fails, an assessment of that component’s relative importance should be done. The failed component may not be immediately required for the reliable operation of the system for the next few days, or even weeks. However, in some cases the entire system is brought down by one component and the only option is to replace it *as soon as possible*.

Purchasing Equipment Immediately

In some cases the fastest solution to a vital failure may be to have personnel go to a

local computer store and purchase a replacement part. This approach is useful only in cases where the part is not technically complicated and replacement can be performed by an “end user”. A good example of this is if a beverage was spilled on the keyboard: rather than wait for service personnel to arrive to plug in a new keyboard, personnel could go to the local computer store and purchase a replacement. This response would also work well for a monitor or printer, however, whenever possible, a qualified service technician should be consulted before disconnecting or installing any equipment. Any other internal or technical equipment should only be serviced by a qualified technician.

Reserving a “Hot Spare”

Typically when a hardware failure occurs a technician will assess the situation and take action to repair or replace the failed component or components. To minimize the possibility of “down time” a “hot spare” can be kept on site or at the service company office. The “hot spare” would be a working computer with all of the components necessary to replace any of the computers in the **SES** system. When the technician arrives to assess the failure, the first operation will be to replace the affected computer with the “hot spare”. Once the damage is repaired, the computer would be replaced, and the “hot spare” would again be set aside.

Although keeping a “hot spare” on site would facilitate a very quick transition, over time the computer acting as the spare may be damaged, become out-dated and eventually become a “wasted” computer. The best option is to have the service company keep a spare always available for you on a contract basis. This would assure you of a working computer whenever you needed it.

Software Protection and Recovery

Any piece of computer equipment can be replaced or repaired, however, if you data is corrupted or lost there are situations where there may be *no way* to recover that information. In that case your **SES** equipment may be fully functional, but essentially useless without the ability to look up resident information or process guests. For this reason data protection is *more important* than equipment maintenance.

Backing Up the System

Just backing up the system is not enough, you need to have an established back up procedure that is followed every time.

The recommended plan is to have two sets of fourteen back up tapes. One set will be kept “off-site”, possibly at the club house, and the other set would be in the gate house. Each night a different tape would be used to perform a complete back up. Once all tapes had been used the set would be exchanged with the set at the club house. Every three months a back up tape will be labeled as a “quarterly backup” and kept for historical purposes (the system will be purged every three months after the quarterly backup).

This back up procedure system would allow you to fall back to any previous day's data for the last twenty-eight days. And if there is a disaster that destroys the gate house (such as a fire) the tapes at the club house would supply data no more that two weeks old.

Restoring Data from Back Up

There are many complications that can arise from restoring previously backed up data, such as overwriting system files and/or restoring to incorrect directories. For this reason it is important that a qualified service technician either performs the data restoration or guides a user though the process over the telephone. Restoring of data should *never* be done without consulting an **SES** technician first, there may be other reasons for the data loss that restoring from back up will not solve.

Total System Failure/Switch to Manual Operation

There may be a time when you experience a total system failure that cannot be immediately be repaired or corrected. This has happened to some **SES** sites during hurricanes and extended power failures.

Procedures for Site Operation with NO **SES** system

The **SES** has the ability to print reports that contain name, address telephone information. These reports can be printed in name or address order and are designed to be kept as a security reference in case the system is inaccessible. A "fresh" report should be printed each month and kept somewhere easily accessible to all personnel.

In addition to the resident reference report, procedures should be developed by security supervisors that would outline how the site will operate in processing people onto the property if there was no access to the **SES** system.

The temporary, manual procedures can efficiently and effectively bridge the gap in system access until the system can be repaired. The procedure may be slightly more inconvenient for the residents, but it is designed as a temporary measure and should maintain a proper level of security.

24 Hour/7Day Service Coverage

The measures outlined above are designed to keep the **SES** system running in a reliable and efficient manner as well as providing for methods of recovery from system failures and damage. If you want further protection, you may want to retain a computer consulting company to provide you with 24/7 coverage. This type of maintenance policy will supply you with a technician anytime you want, twenty-four hours a day, seven days a week. They also usually have a response time of two to four hours.

The Feick Corporation does not offer this service and currently is not affiliated with any company that does offer this. If you wish to pursue this type of coverage, we would recommend finding a reputable company in your area that can provide this to you. We would then meet with the

covering technician and brief them on the system and how it operates.

Summary

Equipment Notes

- ◆ Check UPS packs yearly for proper operation.
- ◆ Install “lightning arrester” power strips.
- ◆ Install telephone surge suppressors.
- ◆ Build an enclosed, ventilated, cooled and filtered computer cabinet.
- ◆ Set up a contract for a “hot spare”.

Software

- ◆ Perform back-ups on a set 28 day rotation.

Manual Operation Procedures

- ◆ Security personnel develop manual (no computer to assist) processing procedures.
- ◆ Print resident information reports on a regular schedule.