

IPC – Data loss protection

Guide / SIMATIC IPC

https://support.industry.siemens.com/cs/ww/en/view/109738084

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

© Siemens AG 2022 All rights reserved

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cert.

Table of contents

Legal information **2**

1 Introduction **4**

1.1 Overview 4

1.2 Principle of operation 4

1.3 Referenced components 4

2 Analysis of possible risk factors **5**

2.1 Overview of possible risk factors 5

2.2 Power failure 5

2.3 Data storage device defects 6

2.4 Operator errors 6

2.5 Manipulation of data 6

2.6 Overheating 6

3 Risk reduction measures **7**

3.1 Overview of suggested protection measures 7

3.2 Preventing data loss from power outages 7

3.2.1 NVRAM 7

3.2.2 Unified Write Filter – UWF 8

3.3 Redundant / uninterruptible power supply (UPS) 10

3.4 RAID system 13

3.5 Backup / restore with SIMATIC IPC Image & Partition Creator 14

3.6 Preventative maintenance and diagnostics with SIMATIC IPC DiagBase / DiagMonitor 15

3.7 IT security concept for additional data protection 16

4 Application examples and applications **17**

4.1 Power supply system with buffer modules for short power outages of multiple seconds 17

4.2 UPS with battery modules for longer power outages 18

5 Summary **19**

6 Appendix **20**

6.1 Service and support 20

6.2 Industry Mall 21

6.3 Links and literature 21

6.4 Change documentation 22

© Siemens AG 2022 All rights reserved

1 Introduction

1.1 Overview

Protecting investments not only means material goods, but also immaterial assets such as data stored on an industrial computer (IPC).

Production downtimes, time spent restoring the function of the industrial computer, or loss of local parameter sets for optimized production processes can lead to serious losses.

Improved protection of these data is therefore an important task for a successful business.

This document addresses risks, such as power outages, that can cause data loss. It presents measures that can help minimize risk and prevent damage. The document is intended as support and contains practical solution suggestions with step-by-step instructions on selected topics.

This will also allow you to recognize and implement opportunities for improvement, and ultimately better safeguard your investments.

1.2 Principle of operation

The document is divided into three major parts:

- Analysis of possible risk factors
- Suggestions for risk mitigation measures
- References to application examples

Some of the suggested risk mitigation measures target multiple risk factors and can be combined with one another.

1.3 Referenced components

Table 1-1 List of hardware and software referenced in this document

Name	Item number
SITOP UPS500S basic unit 15 A with USB port	6EP1933-2EC41
SITOP UPS1600, 24 V/20 A with USB port	6EP4136-3AB00-1AY0
SITOP BAT1600 battery module 12 Ah, Pb	6EP4135-0GE00-0AY0
SITOP PSU8600, 3-phase 24V DC power supply 20A/4X5A with PN interface	6EP3436-8MB00-2CY0
SITOP PSU8600, 3-phase 24V DC power supply 40A/4X10A with PN interface	6EP3437-8MB00-2CY0
SIMATIC IPC Image & Partition Creator V3.6 • Software on USB flash drive • Software and license for download	 6ES7648-6AA13-6YA0 6ES7648-6AA83-6YA0
SIMATIC IPC DiagMonitor V5.1 • Software on USB flash drive • Software and license for download	 6ES7648-6CA15-1YX0 6ES7648-6CA85-1YX0
SIMATIC IPC DiagBase	See link \4\

The components listed here can be obtained through the Siemens Industry Mall or SiePortal.

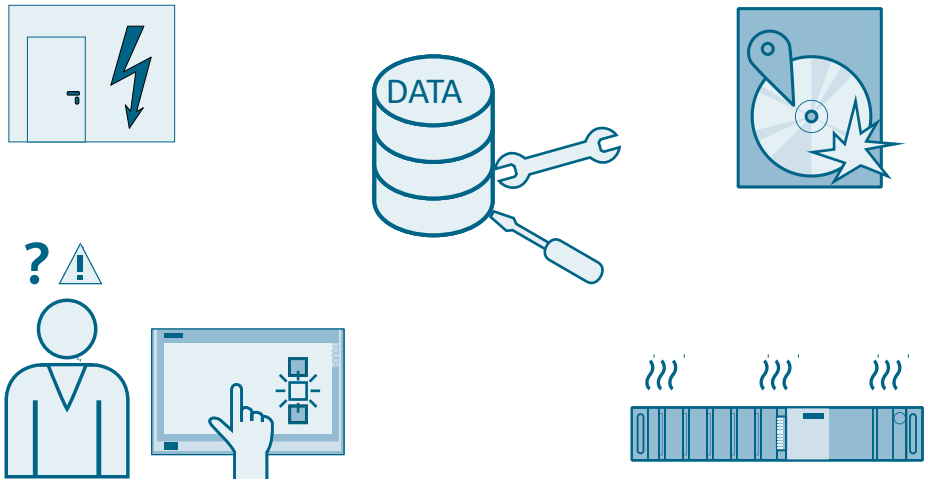
© Siemens AG 2022 All rights reserved

2 Analysis of possible risk factors

2.1 Overview of possible risk factors

The risk of data loss depends on various factors.

Figure 2-1 Risk factors that can lead to data loss



The Figure above shows the following example risk factors.

- Power outages
- Manipulation of data
- Data storage device defects
- Operator error
- Overheating
- & more

These factors are described in greater detail in chapters 2.2 through 2.6.

2.2 Power failure

Power outages in a plant can cause production downtimes and data loss. Such events run the gamut from brief power fluctuations and surges on the order of a few milliseconds (e.g. when turning on large capacitive/inductive loads) to a complete power failure if, for example, the fuse on a power circuit trips, or due to unstable supply from the grid operator.

Short fluctuations in the power supply and power losses of a few milliseconds can be smoothed out by hardened IPC power supplies. When bridging a power failure over a longer time frame, however, even the best power supply unit reaches its limits.

Data stored in the volatile memory (RAM) when the voltage fails will be lost. If a write operation takes place on a storage medium at the moment of the power failure, there is a risk that the data will be incompletely written and thus unusable.

© Siemens AG 2022 All rights reserved

2.3 Data storage device defects

A data storage device has a certain service life in which trouble-free operation can be expected. But a data storage device can still be damaged by excessive thermal mechanical or electrical strain.

Hard disks with rotating magnetic platters can write large volumes of data, but they are sensitive to mechanical shocks and vibrations. Flash storage media on the other hand are less sensitive to mechanical shocks and vibrations, but they can only write a limited amount of data during their lifetime. Frequent write/delete operations thus bring about defects in flash storage media more quickly. Data stored in this range will be lost.

2.4 Operator errors

Even when everything is running from a technical perspective and the IPC is used within its normal parameters, operator errors cannot be ruled out. Behavior patterns that users repeat daily quickly become routine and with this, a potential risk.

Tiredness or lack of focus can lead to operator error. No sooner is a security prompt answered with "Yes", or an operator action performed without thinking, than are vital data deleted.

2.5 Manipulation of data

Besides accidental deletion of data due to operator error, damage can also be caused by unauthorized access. If office and production networks are connected directly, then little stands in the way of malware in the form of viruses and trojans. These are just as much of a threat for the data on an IPC as weak access security or the use of default passwords. These risks should be minimized.

2.6 Overheating

When installing an IPC in a control cabinet, attention should be paid to the installation site and ventilation in order to ensure sufficient heat dissipation during operation. High temperatures cause more intense thermal strain on electronic components, and thus sooner times to failure.

Even the failure of a fan often causes increased temperatures inside of IPC cases. This alone won't cause data loss, but all the components in the IPC's innards are subjected to increased thermal strain. This can cause computing performance sacrifices as the CPU throttles its frequency and premature aging of components; the service life of individual components becomes shortened.

© Siemens AG 2022 All rights reserved

3 Risk reduction measures

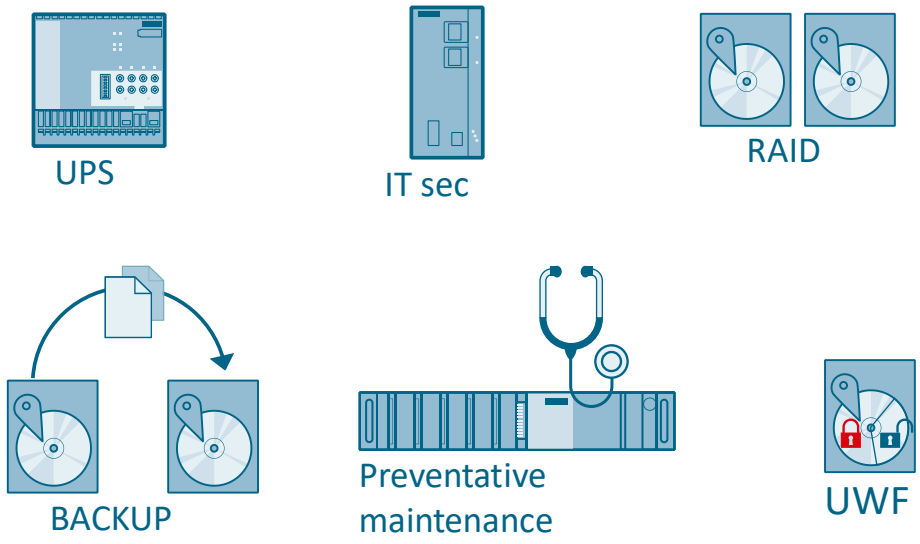
3.1 Overview of suggested protection measures

IPCs already have a high degree of system availability, giving them better data availability than office PCs in an industrial environment. But reliable operation in industrial environments on its own is not enough to guarantee data availability. Therefore, this chapter explains possible measures that can minimize your risk.

A robust IPC offers a good platform for reliable and stable data processing in industry environments. Devices and spare parts are available for long periods of time. High system availability can be achieved with robust components and redundantly designed subsystems.

As illustrated in Figure 3-1, we can build on this with various measures to reduce the risks covered in chapter 2.1.

Figure 3-1: Risk reduction measures



The measures presented either reduce the risk of damage occurring or swift and seamless restoration of lost data. By combining multiple measures, data can be more effectively protected against loss or tampering.

3.2 Preventing data loss from power outages

This chapter discusses technical solutions to prevent data loss in the event of a power outage.

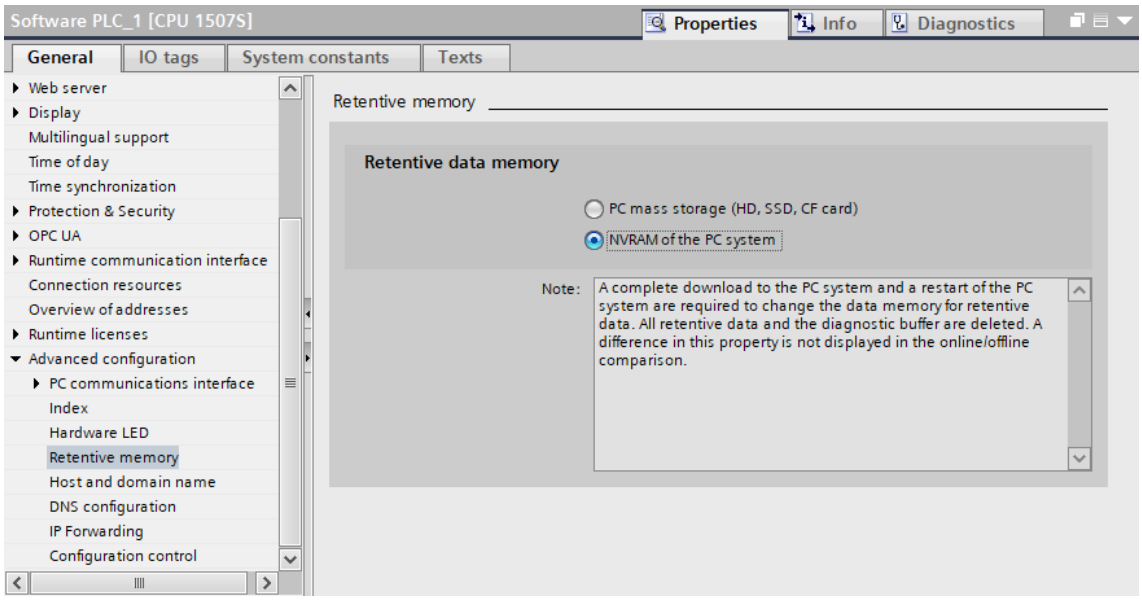
Measures for stabilizing the current and/or improving the availability of the power supply are considered in chapter 3.3.

3.2.1 NVRAM

NVRAM stands for non-volatile random access memory. NVRAM is either a magnetoresistive RAM (MRAM) or a battery-buffered static RAM (SRAM). Like traditional RAM, NVRAM can be used for read and write operations. Unlike RAM, however, data stored in NVRAM remain after power is lost. One use of NVRAM is to save process data from a software PLC.

© Siemens AG 2022 All rights reserved

Figure 3-2: NVRAM usage settings in TIA Portal



If the mains power fails, the power supply sends a signal to the board electronics. It switches off all unnecessary components within a few milliseconds. The power supply still delivers enough residual energy for data backup. After power is restored, the stored data from the controller are available once again.

The NVRAM in SIMATIC IPCs is usually between 128 KB and 512 KB in size. If the IPC does not have NVRAM or the volume of data to be backed up exceeds the free space in the NVRAM, then data must be backed up to an internal data storage device. In this case, however, an uninterruptible power supply with buffer capacity is required. See chapter 3.3.

3.2.2 Unified Write Filter – UWF

The Unified Write Filter (UWF) is the successor to the Enhanced Write Filter (EWF) in Windows XP and Windows 7. It makes it possible to give write protection to data storage devices and partitions. Write operations to the data storage device are re-routed into a part of the RAM with a virtual overlay. See Figure 3-3.

If UWF write protection is activated, no more data can be written to the data storage device or partition. This protects the data stored there from being overwritten.

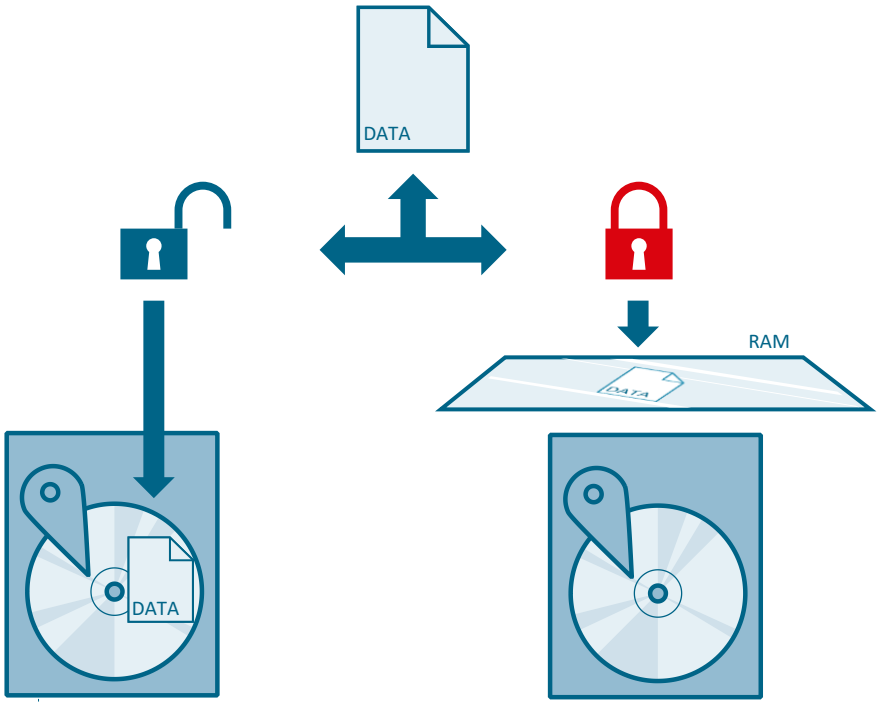
Data from applications that still want to write to the data carrier are instead stored in the IPC's RAM. This process is transparent to the running applications, such that they are indifferent to where the data are stored.

IPC restart

Restarting the IPC causes all data written to the data storage device after activation of write protection to be discarded. The data from RAM are lost. This resets the IPC system to its state at the time at which write protection was activated.

© Siemens AG 2022 All rights reserved

Figure 3-3: Principle of the Unified Write Filter



© Siemens AG 2022 All rights reserved

Making permanent changes

If permanent changes to the protected drive or protected partition are required, the UWF can be temporarily deactivated while the necessary changes are made.

Type of data protection

This type of data protection is particularly suitable for systems where no changes need to be made to the system configuration after a certain point in time, or whose process data and log files are stored on a separate drive or partition.

The UWF is available for the following Microsoft operating systems:

- Windows 10 Enterprise,
- Windows 10 IoT Core,
- Windows 10 IoT Enterprise

For SIMATIC IPCs, the following is a partial list of available operating systems with UWF:

- Windows 10 IoT Enterprise 2019 LTSC
- Windows 10 IoT Enterprise 2016 LTSB

More information can be found on the operating system vendor websites (see reference \5\).

Note

The function is available in the Windows Embedded Standard 7 operating system under the name Enhanced Write Filter (EWF).

Like UWF, EWF makes it possible to give write protection to data storage devices and partitions.

3.3 Redundant / uninterruptible power supply (UPS)

All SIMATIC IPCs work with an integrated industrial power supply for safe current that is protected from grid interference (up to 20 ms per NAMUR).

With SITOP power supplies, a distinction is made between direct current (DC) and alternating current (AC).

- DC power supply
- AC power supply

A separate DC power supply is typically used when an IPC runs on 24 V DC.

SITOP power supplies contain buffer capacitors and can bridge outages in the multi-millisecond range. Longer outages can be bridged with an additional SITOP UPS500S, a UPS with capacitor technology. Depending on the load, these can deliver power for minutes.

To ride out longer outages or continuously stabilize grid power, the SITOP UPS1600 uninterruptible power supply can be used with the additional BAT1600 battery modules. These will provide power to any devices connected to them for a matter of hours in the event of grid failure.

Often UPSs have the ability to poll the status of the grid power and the charge status of the battery / remaining UPS buffer time. If the UPS provides this information via a USB port, an IPC can analyze this information directly.

The capacity of the energy storage of the UPS is an important parameter in this case. Energy reserves should be dimensioned appropriately so that you can safely close open programs and automatically shut down and power off the IPC.

Power supplies from the SITOP series are one suitable option for 24 V DC power supply to SIMATIC IPCs. They are available in 1- and 3-phase variants. With the addition of the SITOP UPS500S uninterruptible power supply, they contribute to the all-around protection of your IPC to safely and quickly shut it down in case the grid power fails.

If higher load currents or longer buffer times are needed, the SITOP UPS1600 uninterruptible power supplies with BAT1600 battery modules provide the capability to bridge power failures lasting on the order of hours.

The SITOP web pages contain decision-making aids for your individual situation (see reference \6\).

© Siemens AG 2022 All rights reserved

Types of energy storage

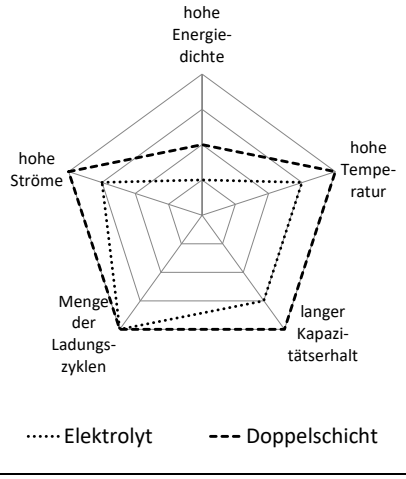
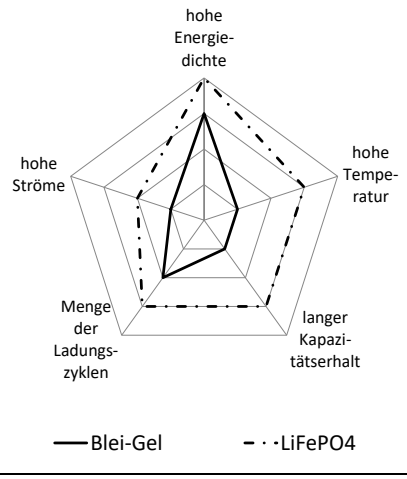
- There are multiple energy storage methods available for storing electrical energy, e.g. electrically-charged capacitors, or
- battery modules (rechargeable batteries) that use electrochemical energy.

These differ with respect to both the storable energy, their longevity and in their characteristic electrical properties.

Table 3-1 shows selected features of energy storage devices.

- Energy density of the energy storage
- Temperature resistance of the energy storage
- Capacity retention over longer times
- Number of possible charge cycles of the energy storage
- Possible currents when charging and discharging the energy storage

Table 3-1: Comparison of different energy storage methods

Capacitors	Battery modules / rechargeable batteries
	

Number of charge cycles

Capacitors can be frequently fully discharged and recharged an almost unlimited number of times. Batteries on the other hand can be damaged by deep discharge. For this reason, rechargeable batteries are discharged and recharged with a suitable charge management system.

High currents

Energy storage devices that use capacitors can quickly take on electrical energy and then discharge it again completely.

High energy density

By contrast, rechargeable batteries that use lead gel, lithium iron phosphate ($LiFePO_4$) or other electrochemical energy storage methods can store greater quantities of energy per unit volume. They are thus able to deliver energy over longer periods of time.

High temperature

Temperature also has effects on the capacity of energy storage devices. Capacitors are generally less sensitive to high temperatures than rechargeable batteries.

Long capacity retention

The capacity of a battery module / rechargeable battery falls as the years pass. Frequent charging cycles and high temperatures exacerbate this aging effect. This can cause the remaining capacity to no longer be sufficient to reliably provide the IPC with power in the event of a power outage.

There are two alternative methods to counteract this effect:

- procurement of an energy storage device with more capacity than originally needed, or
- regular review of available capacity and early replacement of the energy storage device.

Which method is better must be checked on a case-by-case basis.

© Siemens AG 2022 All rights reserved

Connection to 3-phase alternating current

Direction connection of UPS solutions with energy storage units to 1- or 3-phase AC networks is also possible. The SITOP PSU8600 power supply system with the BUF8600 buffer modules or the UPS8600 UPS module and BAT8600 battery modules offers a reliable 24 V DC supply for the IPC in this use case (see references \7\ and \8\).

IPCs with integrated, redundant AC power supply

To guarantee the power supply of an IPC even if a power supply unit fails, SIMATIC rack PCs can be outfitted with an additional redundant power supply unit. If one of the two power supply units fails, the remaining power supply unit continues to deliver current to run the SIMATIC IPC. The SIMATIC IPC will also generate an audible warning signal.

The condition of the power supply units can be diagnosed locally on the SIMATIC IPC with the SIMATIC IPC DiagBase diagnostic software or SIMATIC IPC DiagMonitor. SIMATIC IPC DiagMonitor can also send an email with a corresponding alarm message. Following this, a service technician can hot-swap the defective power supply unit and restore the power supply redundancy. The SIMATIC IPC must not be shut down while the power supply unit is being replaced. The result is no downtime.

Figure 3-4



© Siemens AG 2022 All rights reserved

3.4 RAID system

In order to prevent the loss of data in the event of the failure of a data storage device, the interconnection of several data carriers has proven its worth. This creates a so-called RAID network. RAID stands for "Redundant Array of Independent Disks". Most RAID levels used are RAID 0, 1 and 5.

Table 3-2: Overview of common RAID levels

RAID level	0	1	5
Strength	Speed	Mirroring	Parity
Minimum number of required data storage devices	2	2	3
Number of defective data storage devices without data loss	0	1	1

A RAID network also helps to prevent data loss in industrial computers. IPCs contain special controllers that are capable of operating the built-in data carriers at RAID 0, RAID 1 or RAID 5 level.

RAID 0 is suitable for demanding requirements on data transfer performance. This is accompanied by a higher risk of data loss. Therefore, it is better to employ RAID 1 or 5 when operating two or more data storage devices. In this mode, it is possible to compensate for the failure of an entire data storage device.

If the RAID controller also has the "hot swap" function, the defective data carrier can be exchanged during operation without interrupting the production processes.

SIMATIC IPCs with RAID options are pre-configured and immediately ready for use on delivery.

Protection against inadvertent deletion is offered by SIMATIC UWF Manager, and by creating regular backups. These will be addressed in the chapters below.

More information on the potential applications of RAID systems in IPCs can be found online in the document "RAID systems in industry". See literature reference \9\.

Figure 3-5: Two disks in RAID 1 array



© Siemens AG 2022 All rights reserved

3.5 Backup / restore with SIMATIC IPC Image & Partition Creator

Another way to protect against data loss is regular data backup. Data are secured in the backup process and brought back in the restore process. The redundant data themselves are referred to as the backup.

Setting the scope of a backup

Before backing up, it is worth considering which data need to be backed up. This ranges from single files or parameters to a backup of all the data on a disk, also known as an image.

Creating a backup schedule

Once you know which data should be backed up, the next step is to decide when and how often a backup is needed. If a backup only has to be created once, manual creation is sufficient. Automatic backup creation is recommended for regular backups.

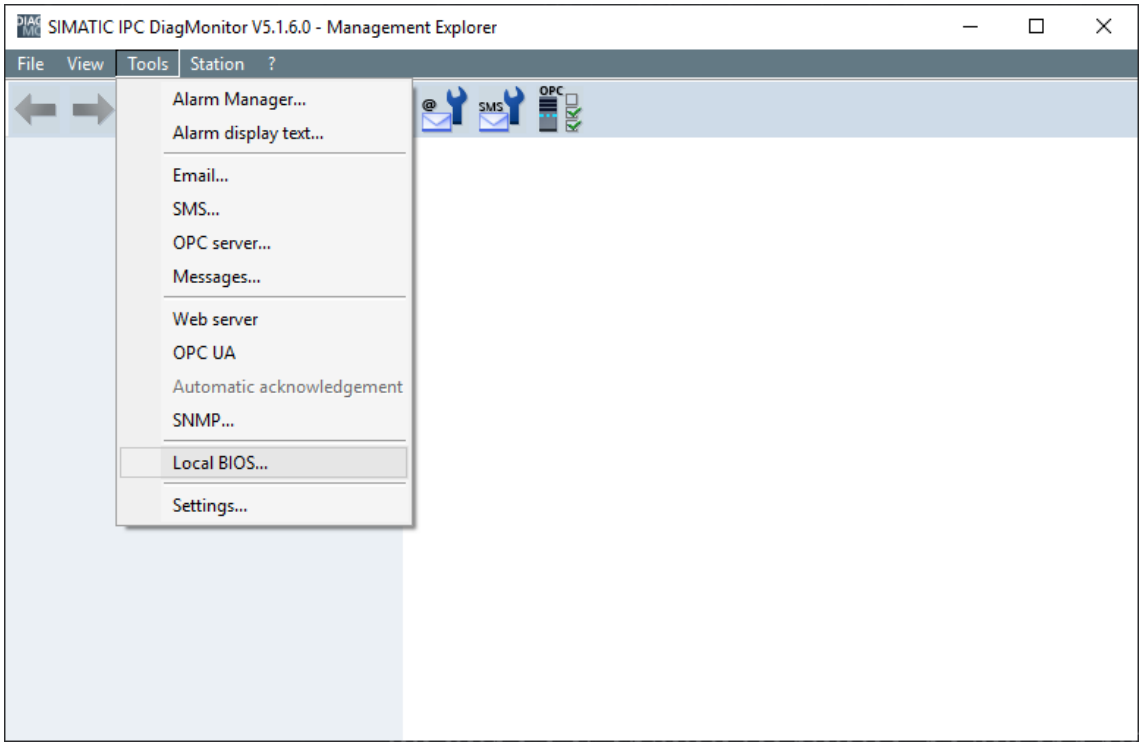
After creating a backup, you should test the restore process at least once. In this way you can familiarize yourself with the process in an emergency and prevent errors.

Backing up BIOS settings

The BIOS of an IPC contains all the important parameters for operation, such as the startup sequence of existing drives, time control of the memory modules, or specific processor functions. Changes to these parameters can affect the performance of the IPC and, in the worst case, prevent the IPC from starting up.

By backing up BIOS settings, the correct parameters can be quickly restored or transferred to a new system. Backup and restore of BIOS settings in SIMATIC IPC is facilitated by the SIMATIC IPC DiagBase and SIMATIC IPC DiagMonitor software.

Figure 3-6: BiosManager dialog window



© Siemens AG 2022 All rights reserved

Backing up single files

Single files such as formulas or log files are often of particular importance. These can be protected against loss by manually copying them to an external data storage device. The Task Scheduler or a similar scheduler is recommended if you plan to carry out this process regularly. These automatically create a copy of the data to be backed up, then save it to remote networked file storage, for example.

Complete system backup

If you intend to back up not just single files but the entire operating system and all the programs and settings on it, it is no longer enough to back up individual files. This task is best accomplished by special backup programs that make a complete copy of the data on an IPC.

The advantage of this method is that, in the event of a disaster or the failure of the data storage device, the data can be fully restored to a replacement system of the same model.

Some backup programs offer the capability to make incremental backups that can keep the initial backup files current. Here, only data that were modified since the last backup are added to the backup. This saves both storage space as well as time.

The "SIMATIC IPC Image & Partition Creator" software is specially optimized for backing up IPCs and contains all the necessary drivers for running their drive controllers.

The application example "Backup and restore of SIMATIC IPCs" provides step-by-step instructions on creating a backup and using it to restore. See reference \10\.

3.6 Preventative maintenance and diagnostics with SIMATIC IPC DiagBase / DiagMonitor

Some events that lead to data loss announce themselves ahead of time. For example, the temperature inside an IPC case rises when a fan fails. This affects the performance of the IPC and the data storage devices. Diagnostic data from the disks are provided via the S.M.A.R.T.[1] interface.

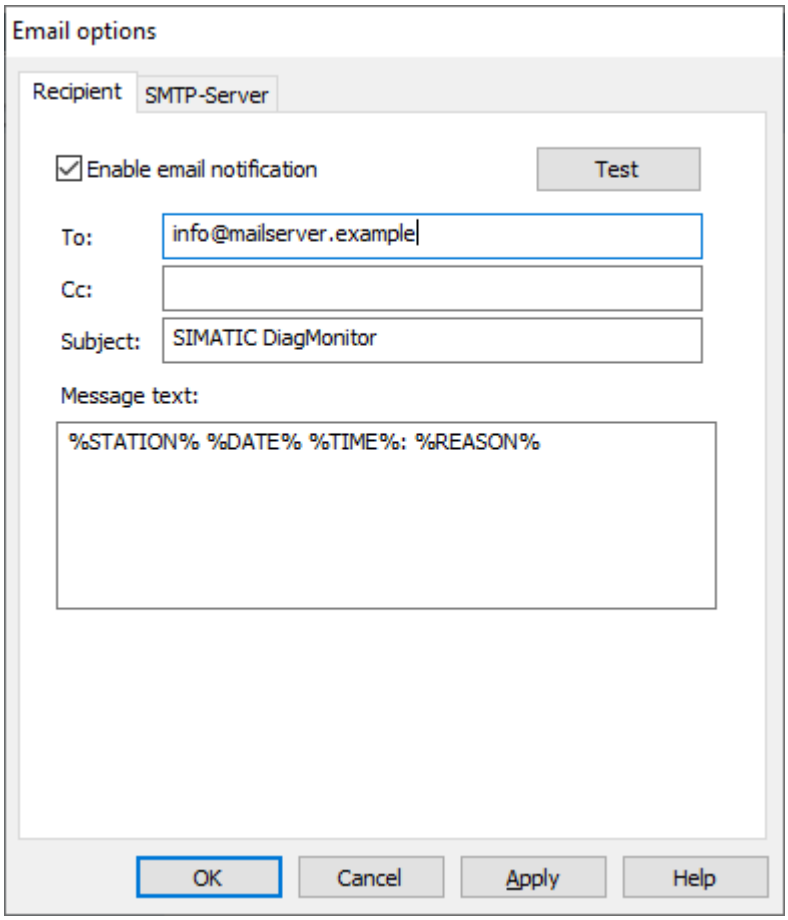
Diagnostic data from the IPC and the disks can be read by a diagnostic program. Upon reaching critical values, the program generates a message that is sent in email form to the relevant maintenance personnel or displayed in the plant's visualization. This allows a maintenance technician to promptly replace the defective fan or replace a data storage device with a new one before it fails due to old age.

SIMATIC IPCs contain the necessary sensors and interfaces, giving the SIMATIC IPC DiagMonitor software the functionality described above.

© Siemens AG 2022 All rights reserved

[1] S.M.A.R.T. = Self-Monitoring, Analysis and Reporting Technology

Figure 3-7: DiagMonitor email options



For support on getting started with SIMATIC IPC DiagMonitor, see the document "SIMATIC IPC DiagMonitor – Getting started" under reference \11\.

More ways of diagnosing SIMATIC IPCs with WinCC (TIA Portal) and WinCC V7 are described in the document "Diagnostic of SIMATIC IPCs". See reference \12\.

3.7 IT security concept for additional data protection

You can counter tampering of data by unauthorized persons with a suitable security concept. Networked systems should always be protected with a firewall and a virus scanner, for example. Non-trivial passwords and multifactor authentication additionally help restrict access to critical functions.

More information on the recommended security settings for IPCs in industrial environments can be found in the document "Security settings for IPCs". It can be accessed online: see reference \13\.

An overview of industrial security topics can be found on the associated homepage. See reference \14\.

Tested software combinations of SIMATIC software, Microsoft operating systems and virus scanners can be found online with the Siemens Compatibility Tool (see reference \15\).

© Siemens AG 2022 All rights reserved

4 Application examples and applications

4.1 Power supply system with buffer modules for short power outages of multiple seconds

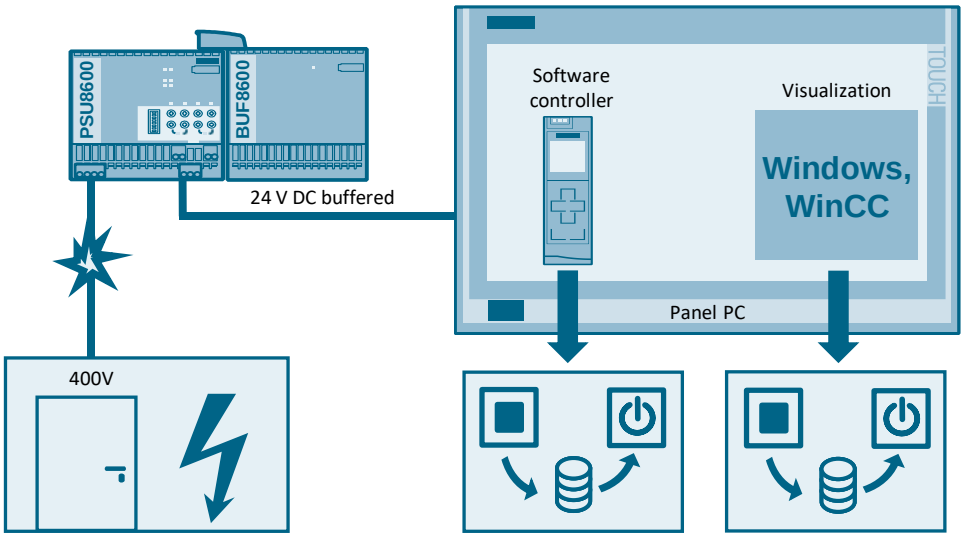
If you only need to bridge short power outages or failures on the order of minutes or seconds, the SITOP PSU8600 power supply system with BUF8600 capacitor-based buffer modules can be used to stabilize the voltage.

The buffer modules store electrical energy and grant an uninterrupted power supply for multiple minutes.

Unlike rechargeable batteries, capacitors can be recharged very fast. This makes them especially suitable for quickly regaining their readiness for the next buffer event. A controller can poll the status of the PSU8600 and the charge state of the BUF8600 buffer module via the integrated Profinet/Industrial Ethernet port. A SIMATIC IPC can automatically shut down if the remaining power drops below a certain threshold.

If buffer times on the order of hours are needed, the SITOP PSU8600 power supply system can be complemented with the UPS8600 UPS module with BAT8600 battery modules.

Figure 4-1: SIMATIC IPC with buffered 24 V DC power supply via SITOP PSU8600 and BUF8600 buffer module



© Siemens AG 2022 All rights reserved

Note

An application example with

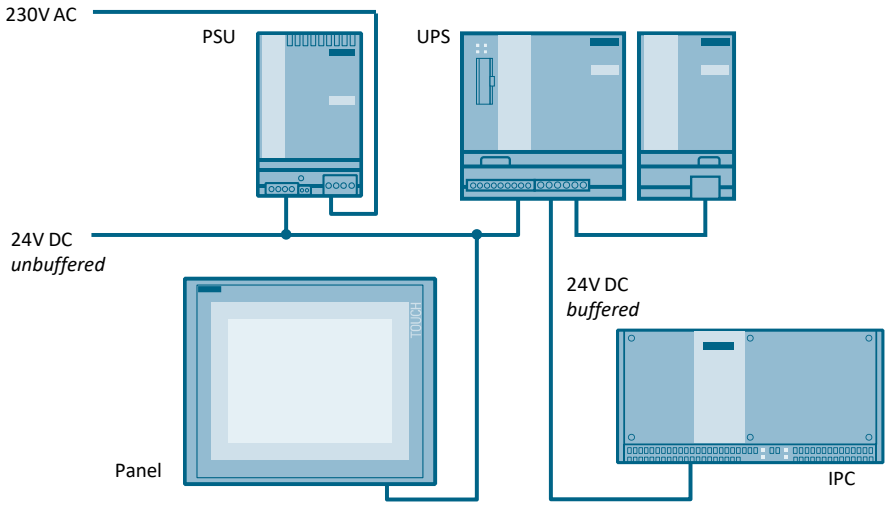
- SIMATIC IPC477D,
- SIMATIC S7-1507S
- SITOP PSU8600 and SITOP BUF8600 buffer module,

including a visualization of the PSU8600 power supply system, is described in the article with article ID 109737962. See reference \16\.

4.2 UPS with battery modules for longer power outages

When a SIMATIC IPC is supplied with power from a UPS, then standardized interfaces can send diagnostic data and warning messages to the SIMATIC IPC for analysis. For example, the SITOP UPS1600 uninterruptible power supply allows the charge status and operating mode of the UPS to be read by the software tool
SITOP Manager. This is powered by the USB connection between the SIMATIC IPC and the UPS, letting you define thresholds at which certain actions will be performed automatically. When the charge state of the battery modules drops below a certain value, for example, SITOP Manager on the SIMATIC IPC can automatically close all applications and shut itself down.

Figure 4-2: SIMATIC IPC with buffered 24 V DC via SITOP UPS1600 with BAT1600 battery module



Note

An application example on buffering SIMATIC IPCs during power outages, and targeted shutdown with SITOP Manager, can be found in the following article:

Article ID 109798562 (reference \17\).

© Siemens AG 2022 All rights reserved

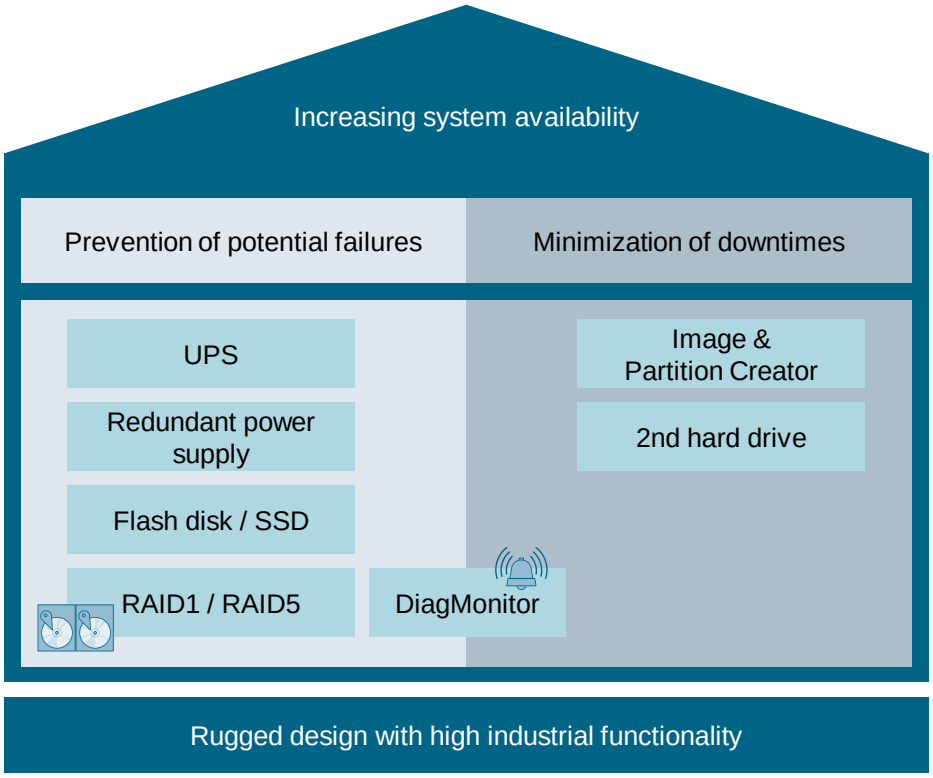
5 Summary

Various measures can be employed to safeguard data. Building on the hardened design of an IPC, a UPS minimizes the risk of data loss resulting from a loss of power. Running two or more data storage devices in a RAID array can protect against data loss in case one data storage device fails, and also allows sustained availability. If the "Hot Swap" function is supported and enabled, a defective data storage device can be replaced while the IPC is turned on and running.

An activated Unified Write Filter can additionally prevent the contents of individual partitions or whole data storage devices from being modified. Not to be overlooked are regular backups, which continue to be essential in protecting against data loss. Analysis of diagnostic information to detect hardware defects before they happen further reduces the risk of data loss resulting from the failure of electrical components.

Even though the risk of data loss can never be completely eliminated, the measures we present above offer many approaches for improving the safety and security of your data. Especially by combining single measures it is possible to create a solution that meets the stringent requirements of data availability in industrial plants.

Figure 5-1



© Siemens AG 2022 All rights reserved

6 Appendix

6.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers
– ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:

siemens.com/SupportRequest

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

© Siemens AG 2022 All rights reserved

6.2 Industry Mall



The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

6.3 Links and literature

Table 6-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109738084
\3\	ASIS - After Sales Information system, Service & Support https://www.siemens.com/asis/
\4\	SIMATIC IPC DiagBase https://support.industry.siemens.com/cs/ww/en/view/29316343
\5\	Unified Write Filter (UWF) https://learn.microsoft.com/en-us/windows-hardware/customize/enterprise/unified-write-filter
\6\	Uninterruptible power supplies from SITOP https://new.siemens.com/global/en/products/automation/power-supply/dc-ups.html
\7\	SITOP PSU8600 20A/4X5A PN power supply https://support.industry.siemens.com/cs/ww/en/pv/6EP3436-8MB00-2CY0/pi?dl=en
\8\	SITOP PSU8600 40A/4X10A PN power supply https://support.industry.siemens.com/cs/ww/en/pv/6EP3437-8MB00-2CY0/pi?dl=en
\9\	RAID systems in industry https://support.industry.siemens.com/cs/ww/en/view/109737064
\10\	Backup and restore of SIMATIC IPCs https://support.industry.siemens.com/cs/ww/en/view/109756568
\11\	SIMATIC IPC DiagMonitor – Getting started https://support.industry.siemens.com/cs/ww/en/view/109479723
\12\	Diagnostic of SIMATIC IPCs https://support.industry.siemens.com/cs/ww/en/view/109478242
\13\	Recommended Security Settings for IPCs https://support.industry.siemens.com/cs/ww/en/view/109475014
\14\	Industrial security homepage https://siemens.com/industrial-security
\15\	Compatibility Tool https://support.industry.siemens.com/compatool/#/main/start

© Siemens AG 2022 All rights reserved

No.	Topic
\16\	Application example – Shutdown SIMATIC IPCs with Software Controller in SITOP PSU8600 Buffer Mode https://support.industry.siemens.com/cs/de/en/view/109737962
\17\	Application example – Buffering SIMATIC IPCs in Case of Power Failure and Targeted Shutdown with SITOP Manager https://support.industry.siemens.com/cs/de/en/view/109798562
\18\	SITOP Manager – the tool for commissioning, engineering and monitoring of SITOP power supplies https://support.industry.siemens.com/cs/ww/en/view/109760607

6.4 Change documentation

Table 6-2

Version	Date	Modifications
V1.2	12/2022	Document revised and updated
V1.1	09/2016	Updated links
V1.0	07/2016	First edition

© Siemens AG 2022 All rights reserved